Gerenciar objetos com ILM

StorageGRID

NetApp
October 03, 2025

Índice

Gerenciar objetos com ILM

Saiba como gerenciar objetos com regras e políticas de ciclo de vida das informações e como usar o bloqueio de objetos do S3 para cumprir com os regulamentos de retenção de objetos.

- "Gerenciamento de objetos com gerenciamento do ciclo de vida das informações"
- "Gerenciando objetos com o S3 Object Lock"
- "Exemplo de regras e políticas ILM"

Gerenciamento de objetos com gerenciamento do ciclo de vida das informações

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

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.

- "Como o ILM opera ao longo da vida de um objeto"
- "O que é uma política ILM"
- "O que é uma regra ILM"
- "Criação de categorias de storage, pools de storage, perfis de EC e regiões"
- "Criando uma regra ILM"
- "Criando uma política ILM"
- "Trabalhando com regras de ILM e políticas de ILM"

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,

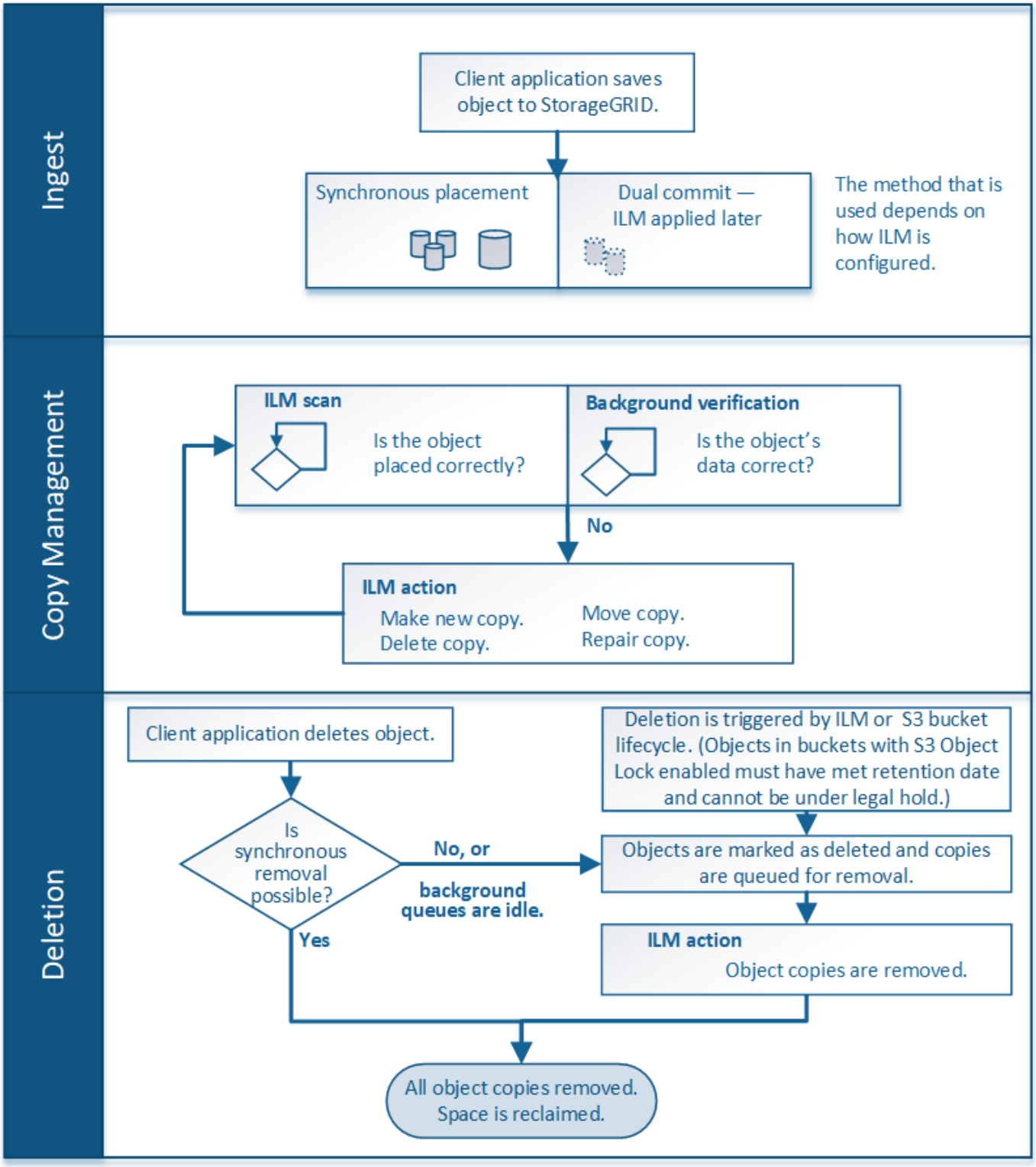
números ou locais de cópias de objetos são necessários, o StorageGRID cria, exclui ou move cópias conforme necessário.

    - 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. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

- **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.



Informações relacionadas

"Monitorizar Resolução de problemas"

Como os objetos são ingeridos

O StorageGRID protege os objetos durante a ingestão, executando o posicionamento síncrono ou executando commit duplo, conforme especificado na regra ILM que corresponde aos objetos.

Quando um cliente S3 ou Swift armazena um objeto na grade, o StorageGRID ingere o objeto usando um destes dois métodos:

- **Colocação síncrona**: O StorageGRID cria imediatamente todas as cópias de objetos necessárias para atender aos requisitos do ILM. O StorageGRID envia uma mensagem de "ingestão bem-sucedida" ao cliente quando todas as cópias são criadas.

  Se o StorageGRID não puder criar imediatamente todas as cópias de objeto (por exemplo, porque um local necessário está temporariamente indisponível), ele enviará uma mensagem "'ingest failed'" para o cliente, ou se recairá a criar cópias de objeto provisórias e avaliar o ILM mais tarde, dependendo da escolha feita quando você criou a regra ILM.

- * Commit duplo*: O StorageGRID cria imediatamente duas cópias provisórias do objeto, cada uma em um nó de armazenamento diferente, e envia uma mensagem "'ingest successful'" ao cliente. O StorageGRID então coloca o objeto em fila para avaliação do ILM.

  Quando o StorageGRID executa a avaliação ILM, ele primeiro verifica se as cópias provisórias satisfazem as instruções de colocação na regra ILM. Por exemplo, as duas cópias provisórias podem satisfazer as instruções em uma regra ILM de duas cópias, mas elas não satisfazem as instruções em uma regra de codificação de apagamento. Se as cópias provisórias não satisfizerem as instruções do ILM, o StorageGRID criará novas cópias de objeto e excluirá quaisquer cópias provisórias que não sejam necessárias.

  Se o StorageGRID não puder criar duas cópias provisórias (por exemplo, se um problema de rede impedir que a segunda cópia seja feita), o StorageGRID não tentará novamente. A ingestão falha.

> Os clientes S3 ou Swift podem especificar que o StorageGRID crie uma única cópia provisória na ingestão especificando `REDUCED_REDUNDANCY` para a classe de armazenamento. Consulte as instruções para implementar um cliente S3 ou Swift para obter mais informações.

Por padrão, o StorageGRID usa o posicionamento síncrono para proteger objetos durante a ingestão.

Informações relacionadas

"Opções de proteção de dados para ingestão"

"Use S3"

"Use Swift"

Opções de proteção de dados para ingestão

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

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 dual 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.

Rigoroso

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 determinado data center.

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

Equilibrado

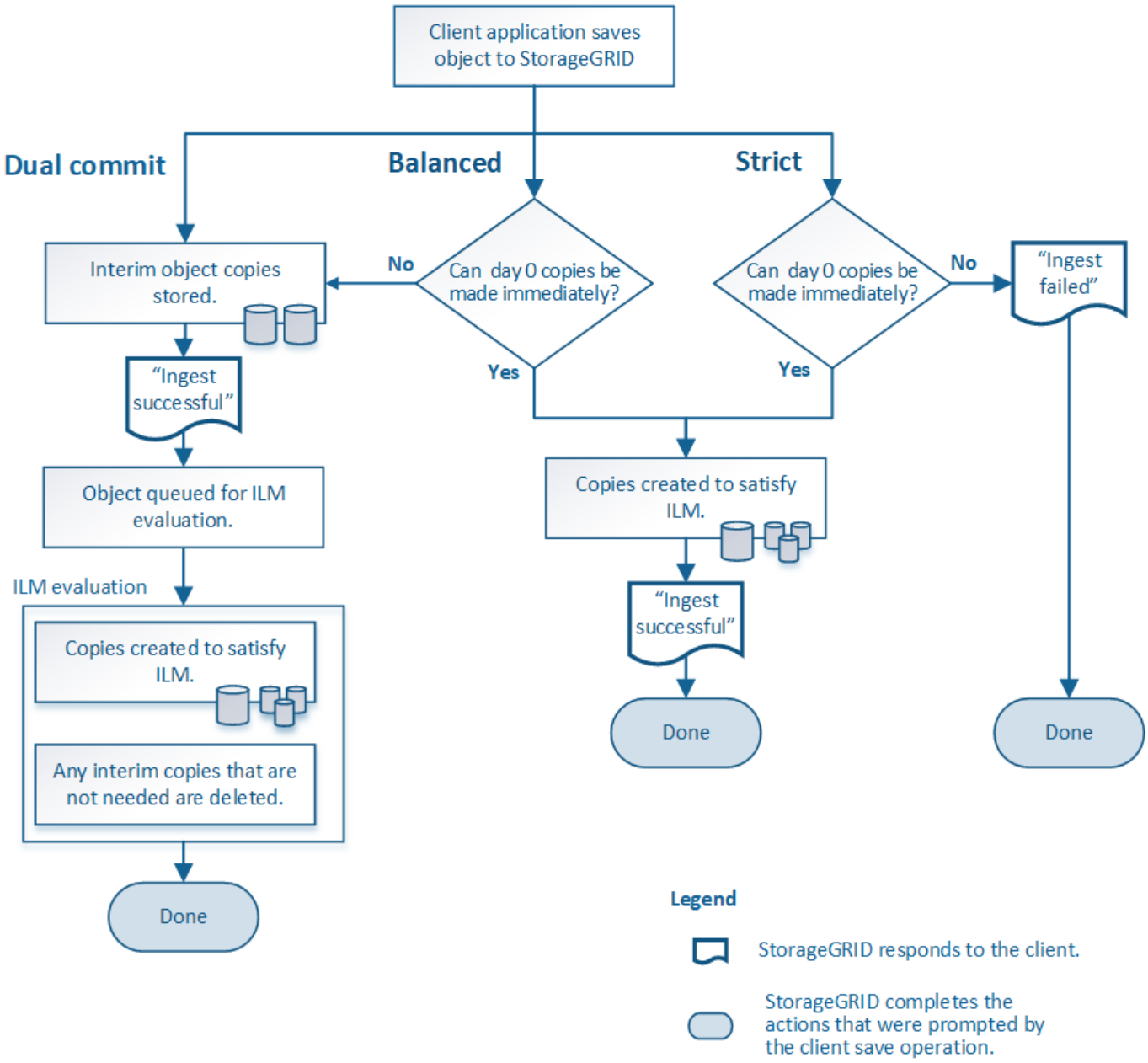
Quando você seleciona a opção equilibrada, o StorageGRID também usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção estrita, se o StorageGRID não puder fazer imediatamente todas as cópias, ele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

Fluxograma de três opções de ingestão

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



Informações relacionadas

"Como os objetos são ingeridos"

Vantagens, desvantagens e limitações das opções de proteção de dados

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.

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 de uso para 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 e 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 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 não for possível fazer alterações de posicionamento necessárias (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 ou 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 exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados 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.
- **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA.

> Antes de selecionar um nível de consistência, leia a descrição completa dessas configurações nas instruções para criar um aplicativo cliente S3 ou Swift. 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

"O que é replicação"

"O que é codificação de apagamento"

"Quais são os esquemas de codificação de apagamento"

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

"Use S3"

"Use Swift"

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

O StorageGRID pode proteger objetos contra perda armazenando cópias replicadas ou armazenando cópias codificadas por apagamento. Você especifica o tipo de cópias a serem criadas nas instruções de colocação das regras do ILM.

- "O que é replicação"
- "Por que você não deve usar replicação de cópia única"
- "O que é codificação de apagamento"
- "Quais são os esquemas de codificação de apagamento"
- "Vantagens, desvantagens e requisitos para codificação de apagamento"

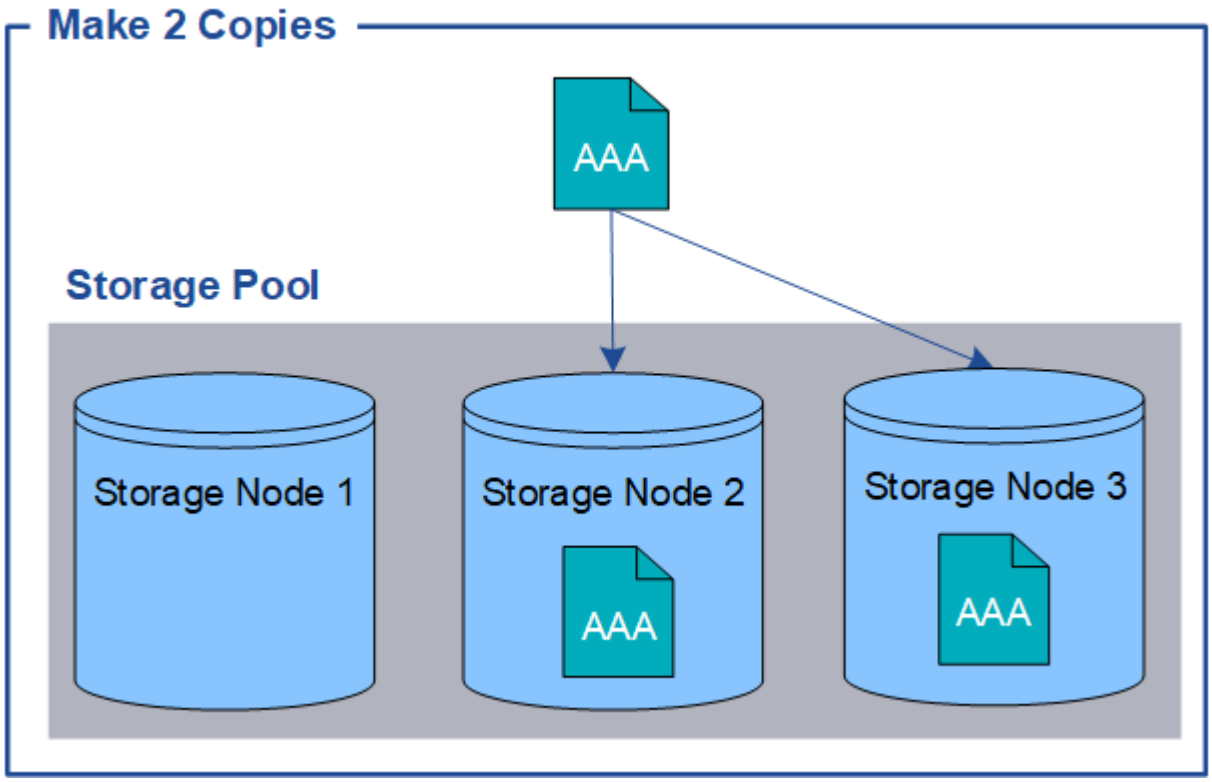
O que é replicação

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 um pool de armazenamento"

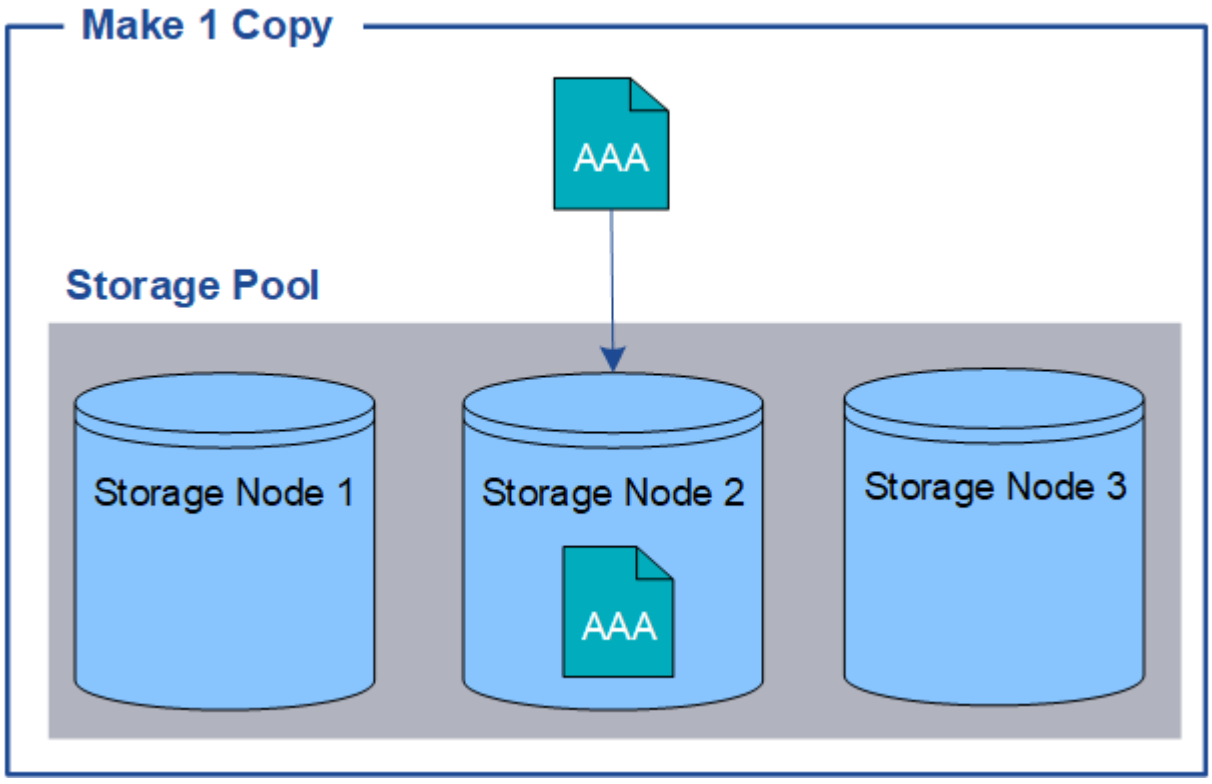
"Uso de vários pools de storage para replicação entre locais"

Por que você não deve usar replicação de cópia única

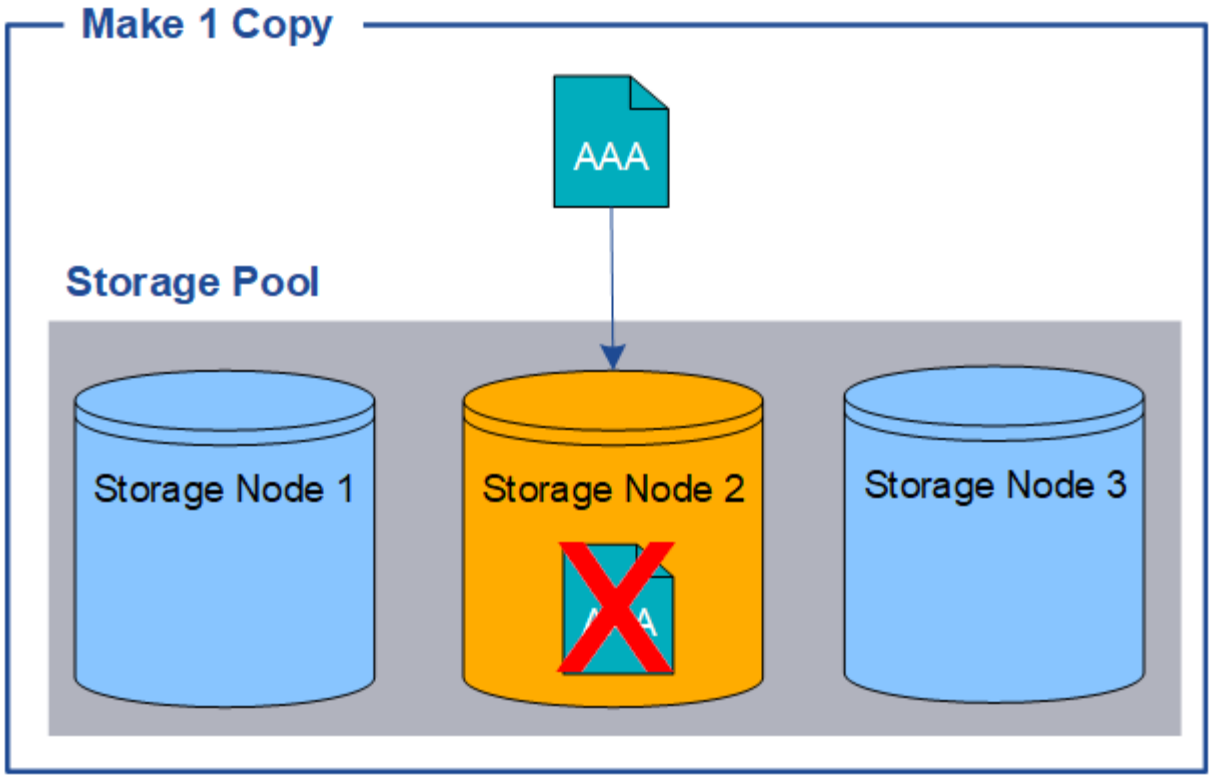
Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de colocação.

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.

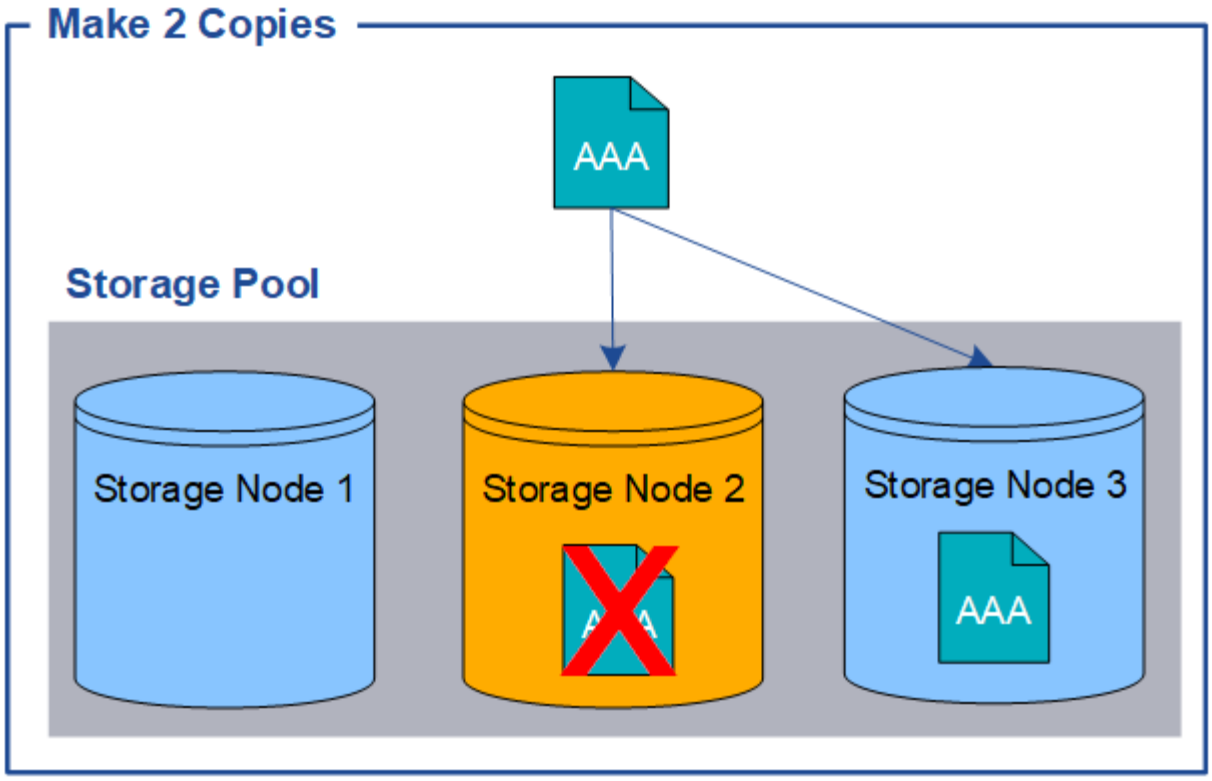
No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contém três nós de storage. Quando um objeto é ingerido que corresponde a essa regra, o StorageGRID coloca uma única cópia em apenas um nó de storage.



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.



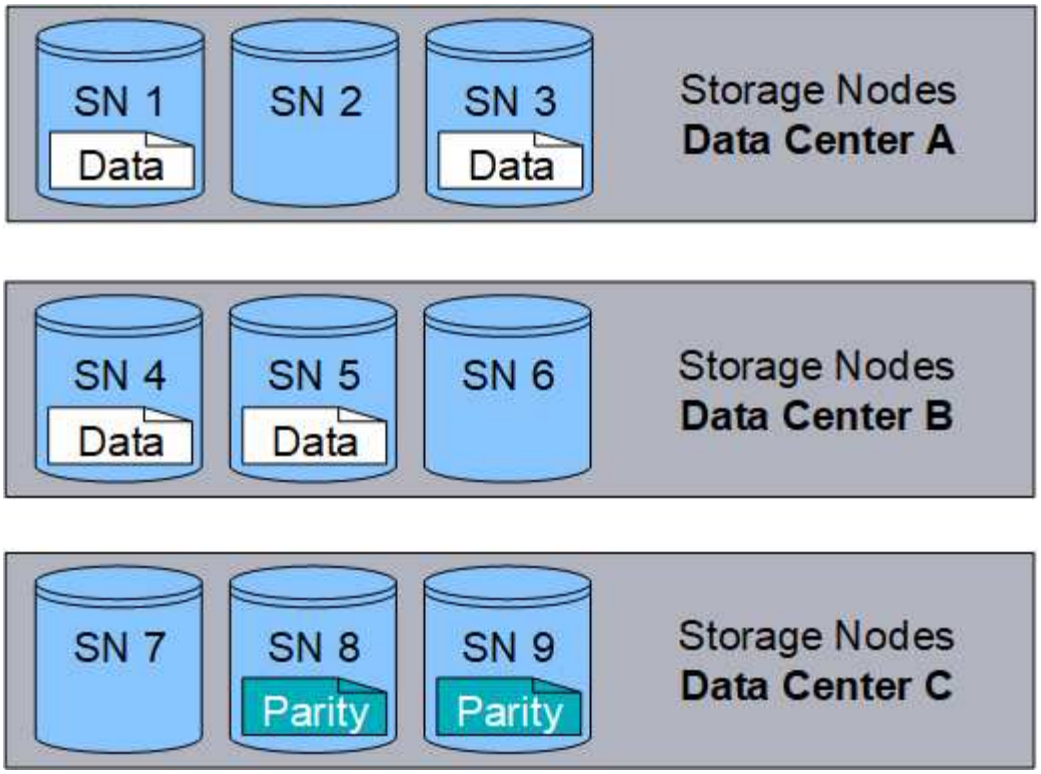
Para evitar a perda de dados de objetos, você sempre deve fazer pelo menos duas cópias de todos os objetos que deseja proteger com a replicação. Se existirem duas ou mais cópias, ainda poderá aceder ao objeto se um nó de armazenamento falhar ou ficar offline.



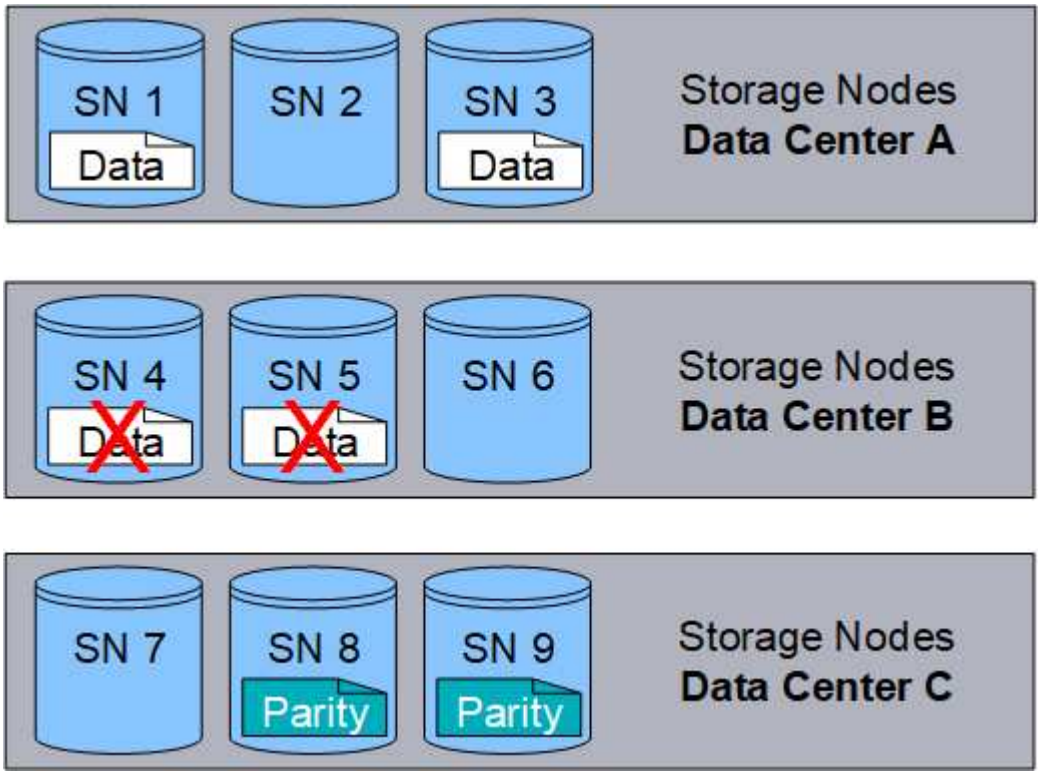
O que é codificação de apagamento

A codificação de apagamento é o segundo método usado pelo StorageGRID para armazenar dados de objetos. Quando o StorageGRID faz a correspondência de objetos a uma regra ILM configurada para criar cópias codificadas por apagamento, ele corta dados de objetos em fragmentos de dados, calcula fragmentos de paridade adicionais e armazena cada fragmento em um nó de storage 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.

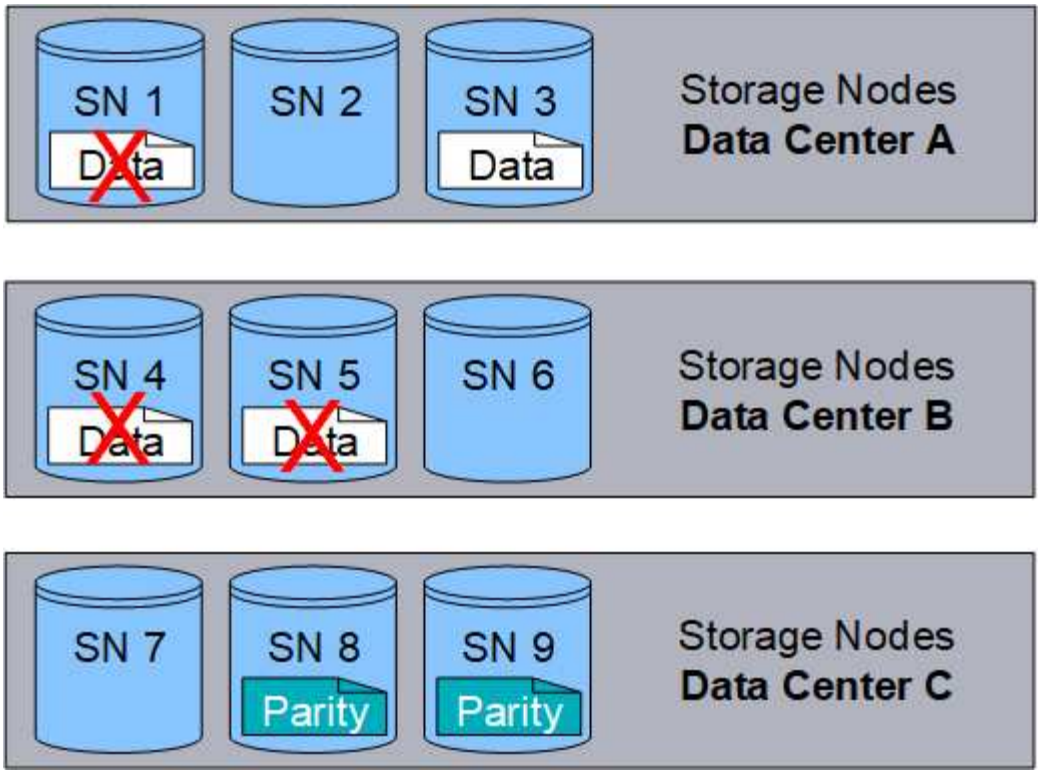
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de apagamento 4-2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados 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 mais de 2 requer um mínimo de nove nós de storage, com três nós de storage em cada um dos três locais diferentes. 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 de data center for perdido, o objeto ainda poderá 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 um pool de armazenamento"

"Quais são os esquemas de codificação de apagamento"

"Configurando perfis de codificação de apagamento"

Quais são os esquemas de codificação de apagamento

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

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

Ao configurar um perfil de codificação de 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 configurar um perfil de 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 o pool de storage padrão, todos os nós de storage ou um pool de storage que inclua o site padrão, todos os sites.
- O pool de storage deve incluir, no mínimo, *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.

Os esquemas de codificação de apagamento com um número menor de fragmentos são geralmente mais eficientes em termos computacionais, pois menos fragmentos são criados e distribuídos (ou recuperados) por objeto, podem mostrar melhor desempenho devido ao tamanho maior do fragmento e podem exigir menos nós sendo adicionados em uma expansão quando mais storage é necessário. (Consulte as instruções para expandir o StorageGRID para obter informações sobre como Planejar uma expansão de armazenamento.)

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 perdas 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 armazenamento 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%
8-2	5	3	15	Sim	25%
6-+3	3	4	12	Sim	50%

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
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, quando *m* tem um valor maior.)
- **Tráfego de rede**: Ao recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total mais alto 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 recomendado um pool de storage com nós de storage _k m_1. 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%

Informações relacionadas

"Expanda sua grade"

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:

- É necessário aumentar o número de nós e locais de storage. Por exemplo, se você usar um esquema de codificação de apagamento de 6 a 3, precisará ter pelo menos três nós de storage em três locais diferentes. Em contraste, se você simplesmente replicar dados de objeto, precisará de apenas um nó de storage para cada cópia.
- Aumento do custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, basta adicionar capacidade de storage em todos os locais onde as cópias de objetos são feitas. 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, você deve adicionar pelo menos nós de storage *k-m*, mas 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, consulte as instruções para expandir o StorageGRID.
- 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 coneta).
- 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.

> Devido à sobrecarga de gerenciamento do número de fragmentos associados a uma cópia codificada por apagamento, não use a codificação de apagamento para objetos de 200 KB ou menos.

- 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.

Informações relacionadas

"Expanda sua grade"

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.

    "Gerenciando objetos com o S3 Object Lock"

- 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.
- 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.

Informações relacionadas

"Gerenciando objetos com o S3 Object Lock"

"Use S3"

"Quais são as instruções de colocação de regras do ILM"

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	Quando **qualquer** das seguintes condições for verdadeira: • A exclusão automática de objetos foi acionada por um dos seguintes eventos: ◦ 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. **Observação:** 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. • Um cliente S3 ou Swift solicita a exclusão e uma ou mais destas condições é verdadeira: ◦ 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)	Quando um cliente S3 ou Swift faz uma solicitação de exclusão e **todas** das seguintes condições são atendidas: • 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 vários 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.

Entendendo o impactos de como o StorageGRID exclui 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.

Você deve estar ciente de que o 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 simplesmente 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 NotFound. 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, você deve fazer um dos seguintes procedimentos:

- **Solicitação de cliente S3**: Especifique o número 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.
- **ILM**: Adicione duas regras ILM à sua política ILM. Use **tempo não atual** como tempo de referência na primeira regra para corresponder às versões não atuais do objeto. Use **tempo de ingestão** na segunda regra para corresponder à versão atual. A regra **hora não atual** deve aparecer na política acima da regra **tempo de ingestão**.

Informações relacionadas

"Use S3"

"Exemplo 4: Regras ILM e política para objetos com versão S3"

O que é uma política ILM

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.

Como uma política ILM avalia objetos

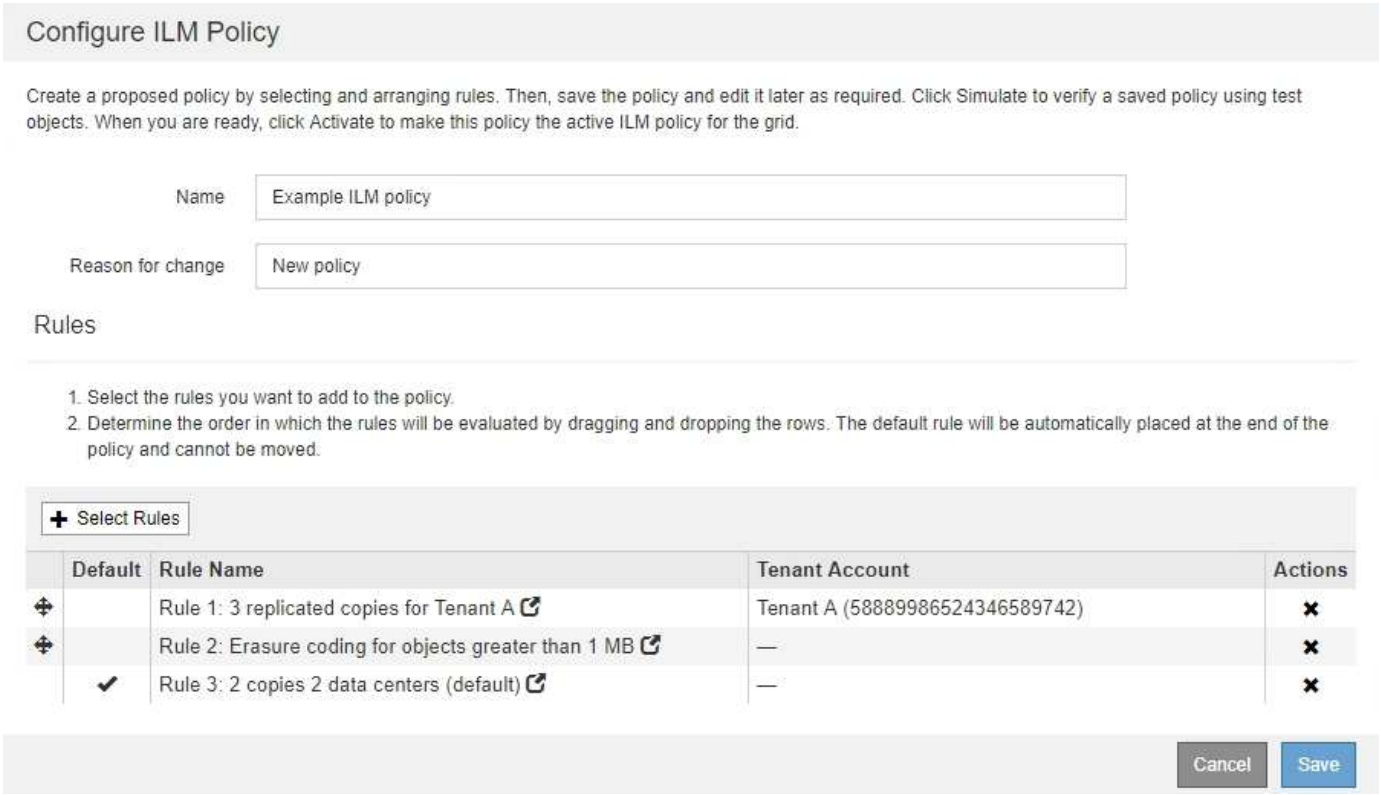
A política de ILM ativa do seu sistema StorageGRID controla o posicionamento, a duração e a proteção de dados de todos os objetos.

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 e não pode usar nenhum filtro.

Exemplo de política ILM

Este exemplo de política ILM usa três regras ILM.

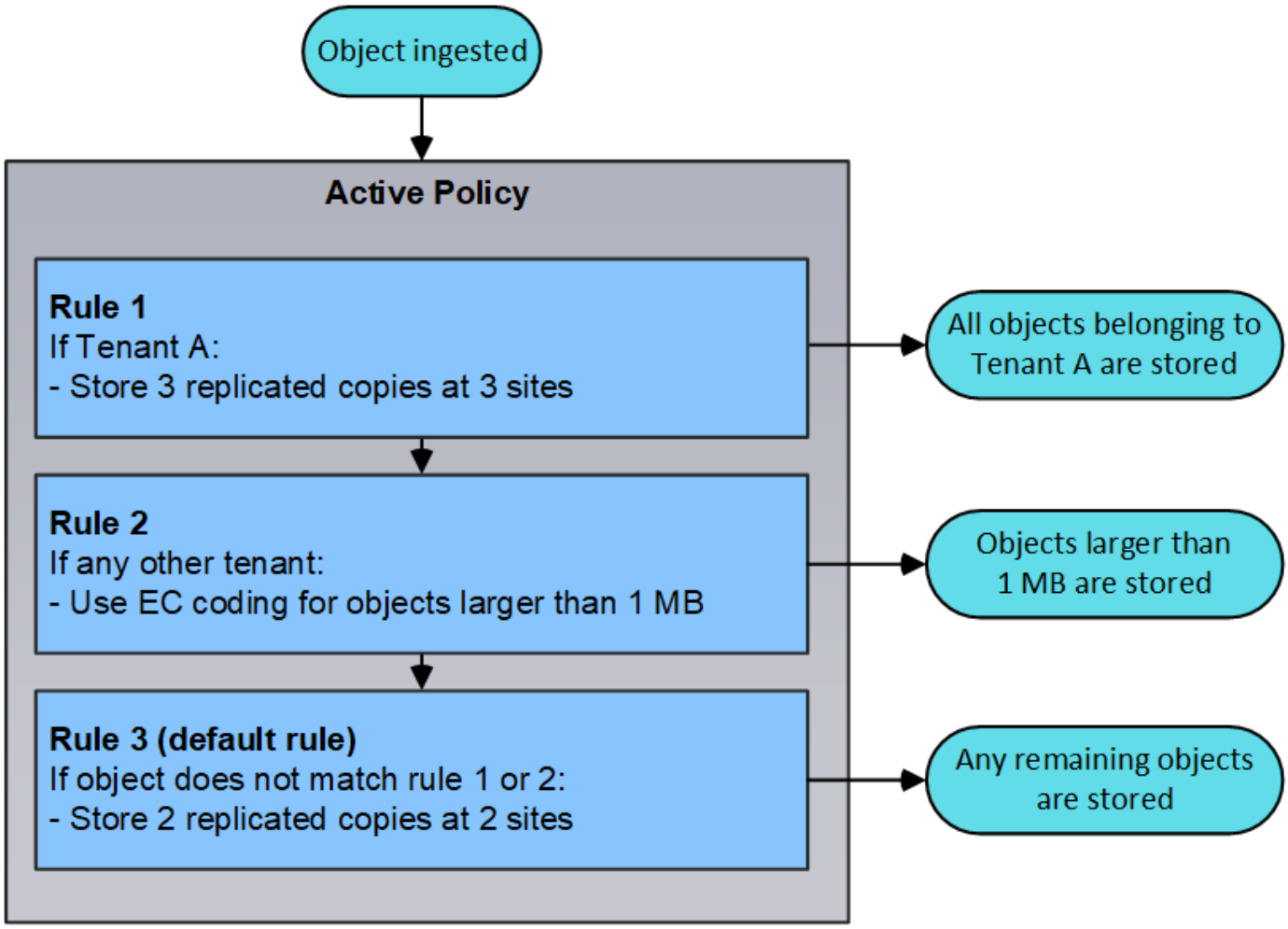


Neste exemplo, a regra 1 corresponde a todos os objetos pertencentes ao locatário A. esses objetos são armazenados como três cópias replicadas em três locais. Os objetos pertencentes a outros inquilinos não são correspondidos pela regra 1, por isso são avaliados em relação à regra 2.

A regra 2 corresponde a 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. A regra 2

não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados em relação à regra 3.

A regra 3 é a última regra padrão da política e não usa filtros. A regra 3 faz duas cópias replicadas de todos os objetos não correspondidos pela regra 1 ou pela regra 2 (objetos que não pertencem ao locatário A com 1 MB ou menos).



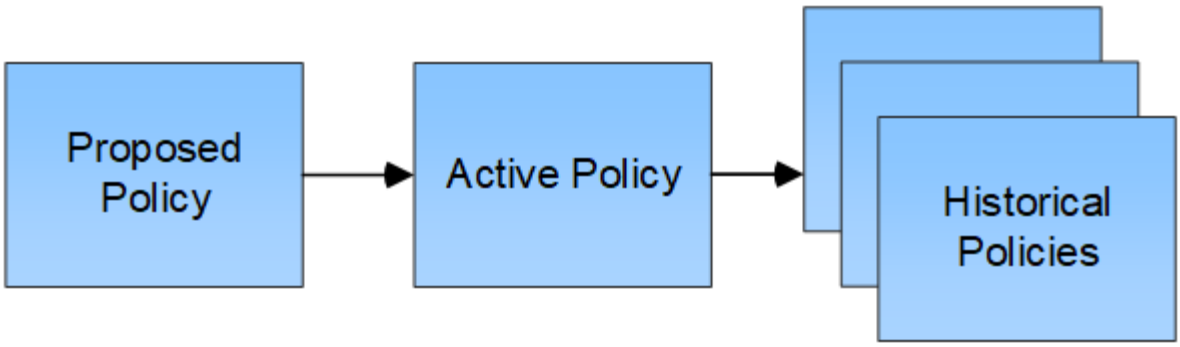
O que as políticas propostas, ativas e históricas são

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 ILM históricas não podem ser eliminadas.



Informações relacionadas

"Criando uma política ILM"

O que é uma regra ILM

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.

As regras do ILM definem:

- Quais objetos devem ser armazenados. Uma regra pode ser aplicada a todos os objetos ou você pode especificar filtros para identificar quais objetos uma regra se aplica. Por exemplo, uma regra só pode se aplicar a objetos associados a determinadas contas de locatário, buckets específicos do S3 ou contentores Swift ou valores específicos de metadados.
- O tipo de armazenamento e a localização. Os objetos podem ser armazenados em nós de storage, em pools de storage de nuvem ou em nós de arquivamento.
- O tipo de cópias de objeto feitas. As cópias podem ser replicadas ou codificadas para apagamento.
- Para cópias replicadas, o número de cópias feitas.
- Para cópias codificadas de apagamento, o esquema de codificação de apagamento usado.
- As alterações ao longo do tempo para o local de armazenamento de um objeto e tipo de cópias.
- Como os dados do objeto são protegidos à medida que os objetos são ingeridos na grade (colocação síncrona ou commit duplo).

Observe que 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. As cópias são distribuídas uniformemente por todos os nós de storage.

Elementos de uma regra ILM

Uma regra ILM tem três elementos:

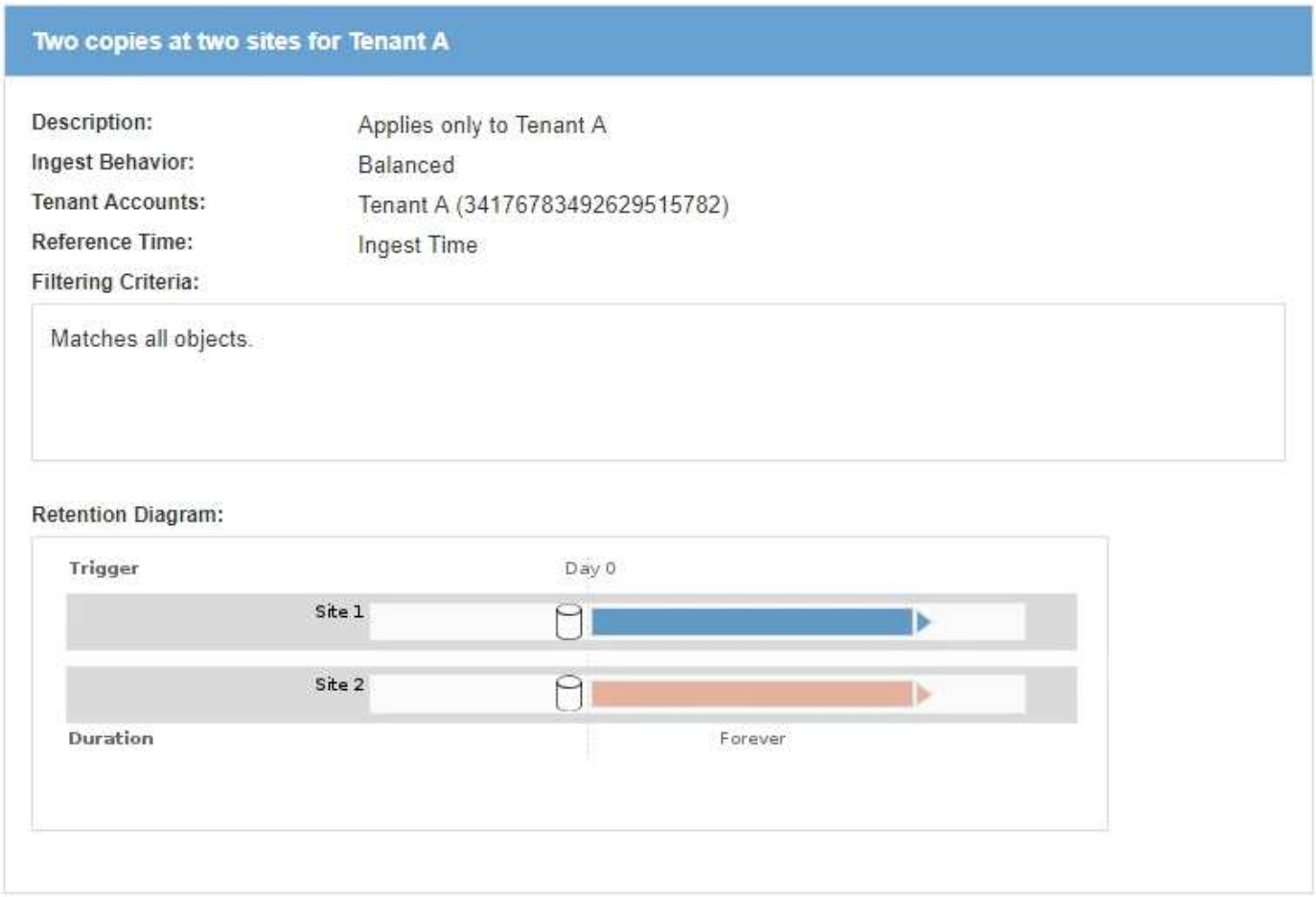
- **Critérios de filtragem**: Os filtros básicos e avançados de uma regra definem a que objetos a regra se aplica. Se um objeto corresponder a todos os filtros, o StorageGRID aplicará a regra e criará as cópias de objeto especificadas nas instruções de colocação da regra.

- **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 define o que acontece quando um cliente S3 ou Swift salva um objeto na grade. 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.

Exemplo de regra ILM

Este exemplo de regra ILM aplica-se aos objetos pertencentes ao locatário A. Ele faz duas cópias replicadas desses objetos e armazena cada cópia em um local diferente. As duas cópias são retidas para sempre, o que significa que o StorageGRID não as apagará 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.

Esta regra usa a opção equilibrada para o 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

"Opções de proteção de dados para ingestão"

"O que é um pool de armazenamento"

"O que é um Cloud Storage Pool"

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

"O que é a filtragem de regras ILM"

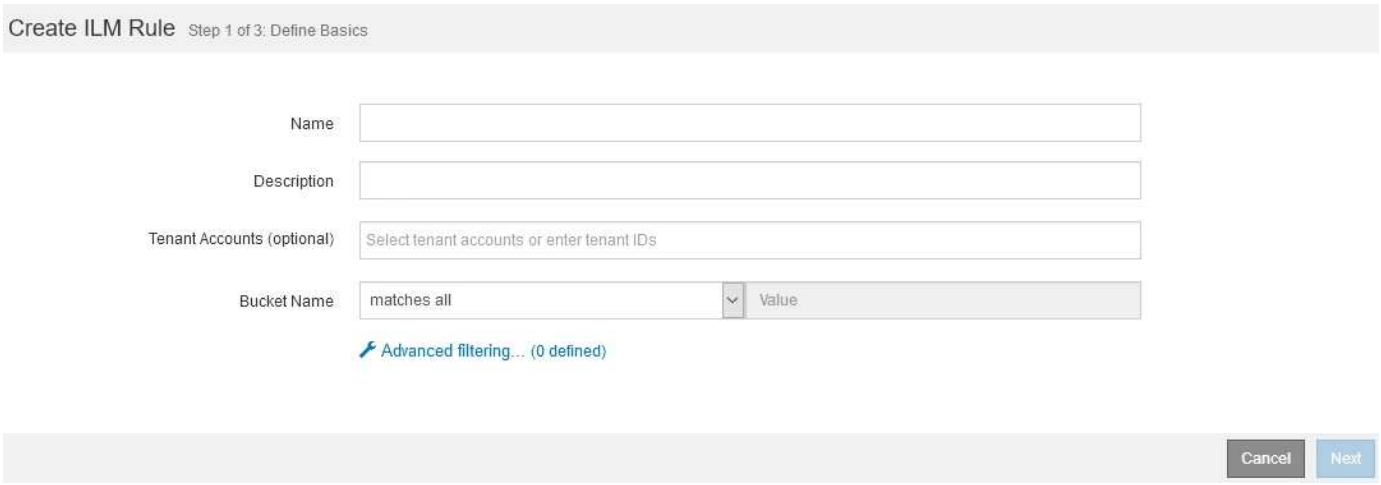
"Quais são as instruções de colocação de regras do ILM"

O que é a 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. Os filtros básicos na página Definir noções básicas do assistente criar regra ILM permitem aplicar uma regra a contas de locatário específicas, buckets específicos do S3 ou contentores Swift, ou ambos.



Esses 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.

A página **Advanced Filtering** do assistente Create ILM Rule fornece 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)
- S3 região do balde (restrição de localização)

- Tamanho do objeto
- Metadados do usuário
- S3 tags de objeto

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 também pode combinar filtros básicos e avançados 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 avançados em cada regra para identificar o tipo específico de objetos aos quais a regra se aplica.

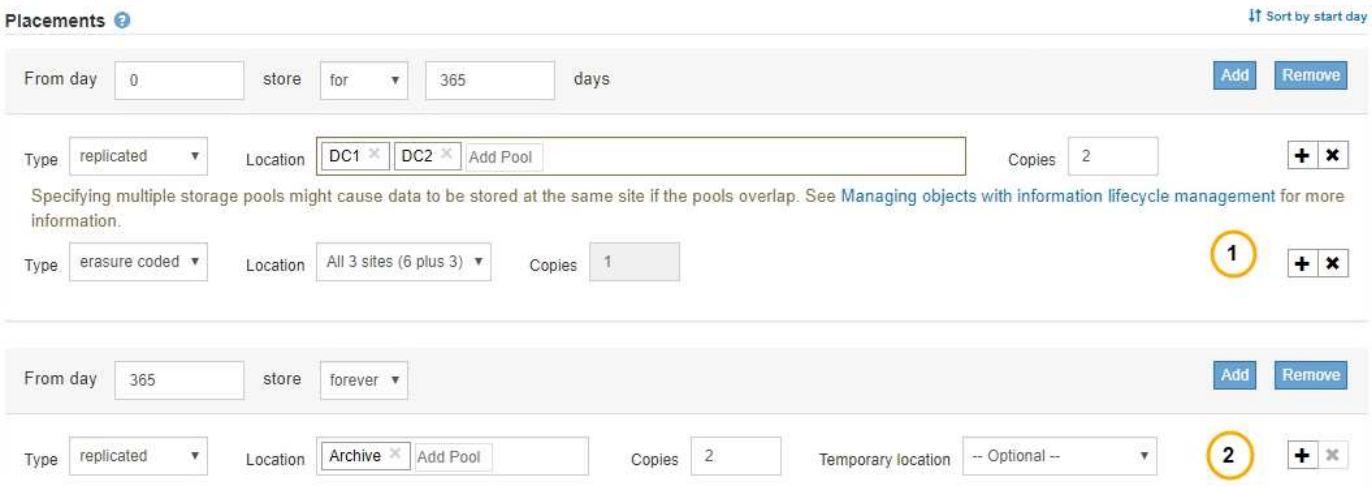
Quais são as instruções de colocação de regras do ILM

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 uma instrução de posicionamento, você especifica quando o posicionamento se aplica (o período de tempo), que tipo de cópias criar (replicadas ou codificadas para apagamento) e onde armazenar as cópias (um ou mais locais de storage). Em uma única regra, você pode especificar vários canais por um período de tempo e instruções de posicionamento por mais de um período de tempo:

- Para especificar mais de um posicionamento de objeto durante um único período de tempo, clique no ícone de sinal de adição ➕para adicionar mais de uma linha para esse período de tempo.
- Para especificar posicionamentos de objetos por mais de um período de tempo, clique no botão **Adicionar** para adicionar o próximo período de tempo. Em seguida, especifique uma ou mais linhas dentro do período de tempo.

O exemplo mostra a página Definir posicionamentos do assistente criar regra ILM.



1	A primeira instrução de colocação tem duas linhas para o primeiro ano: 1. A primeira linha cria duas cópias de objeto replicadas em dois locais de data center. 2. A segunda linha cria uma cópia codificada por apagamento de mais de 6 3 usando três locais de data center.
2	A segunda instrução de colocação 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.

Criação de categorias de storage, pools de storage, perfis de EC e regiões

Antes de criar as regras de ILM para o seu sistema StorageGRID, você deve definir locais de storage de objetos, determinar os tipos de cópias desejadas e, opcionalmente, configurar regiões S3.

- "Criação e atribuição de notas de armazenamento"
- "Configurando pools de armazenamento"
- "Usando Cloud Storage Pools"
- "Configurando perfis de codificação de apagamento"
- "Configurar regiões (opcional e apenas S3)"

Criação e atribuição de notas de armazenamento

Os graus de armazenamento identificam o tipo de armazenamento usado por um nó de armazenamento. Você pode criar graus de storage se quiser que as regras de ILM coloquem certos objetos em determinados nós de storage, em vez de em todos os nós no local. Por exemplo, você pode querer que certos objetos sejam armazenados em seus nós de storage mais rápidos, como dispositivos de storage all-flash StorageGRID.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Se você usar mais de um tipo de armazenamento, você pode criar opcionalmente um nível de armazenamento para identificar cada tipo. A criação de classes de armazenamento permite selecionar um tipo específico de nó de armazenamento ao configurar pools de armazenamento.

Se o nível de storage não for uma preocupação (por exemplo, todos os nós de storage são idênticos), você poderá ignorar este procedimento e usar o nível de storage padrão de todos os nós de storage ao configurar pools de storage.

Quando você adiciona um novo nó de storage em uma expansão, esse nó é adicionado ao nível de storage padrão de todos os nós de storage. Como resultado:

- Se uma regra de ILM usar um pool de storage com o nível todos os nós de storage, o novo nó poderá ser usado imediatamente após a conclusão da expansão.
- Se uma regra de ILM usar um pool de armazenamento com um grau de armazenamento personalizado, o novo nó não será usado até que você atribua manualmente o grau de armazenamento personalizado ao nó, conforme descrito abaixo.

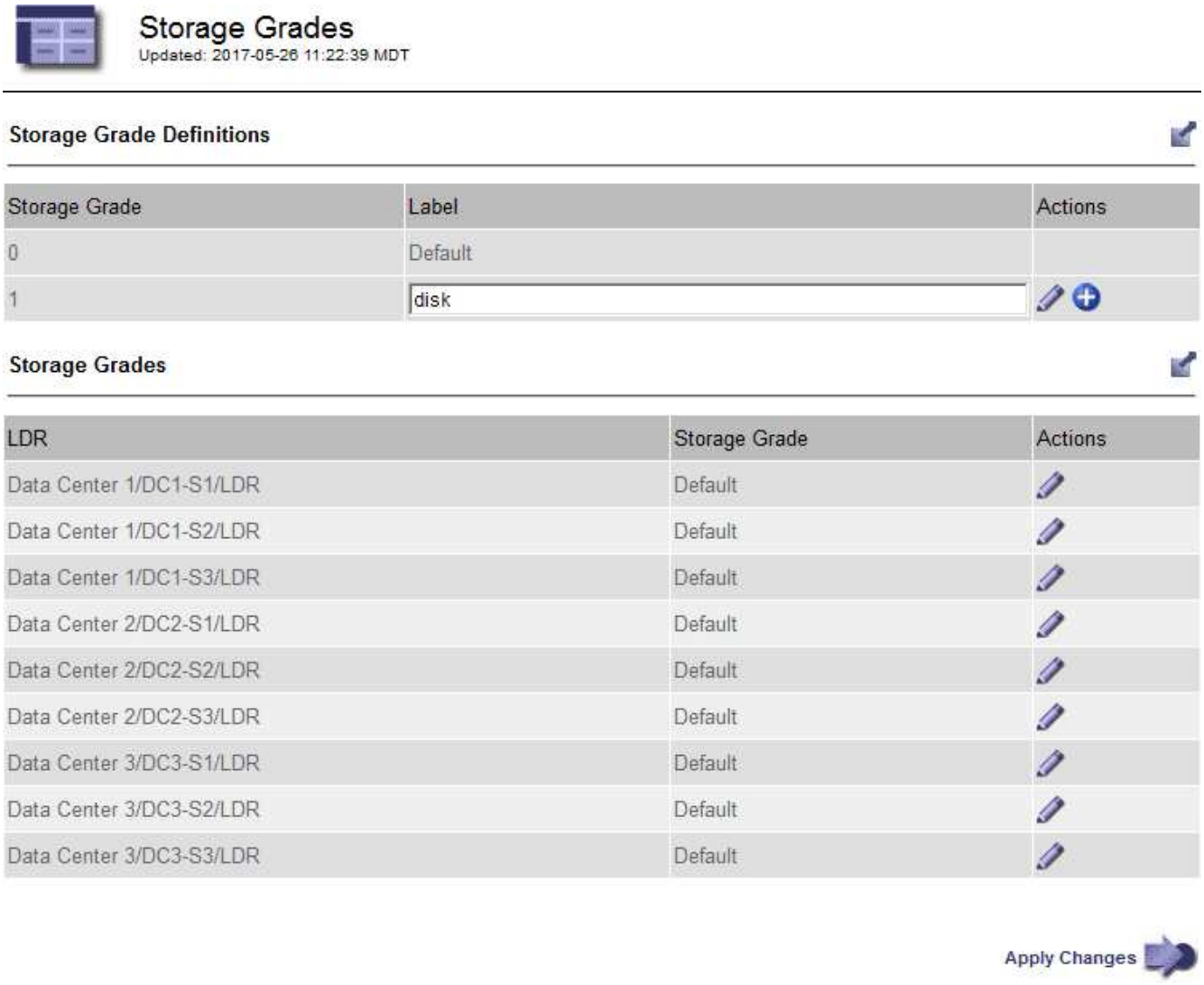
> Ao criar classes de armazenamento, não crie mais classes de armazenamento do que o necessário. Por exemplo, não crie um nível de storage para cada nó de storage. Em vez disso, atribua cada nível de storage a dois ou mais nós. Os graus de armazenamento atribuídos a apenas um nó podem causar backlogs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

Passos

1. Selecione **ILM** > **classes de armazenamento**.
2. Criar um grau de armazenamento:

   a. Para cada grau de armazenamento que você precisa definir, clique em **Insert** para adicionar uma linha e insira um rótulo para o grau de armazenamento.

      O grau de armazenamento predefinido não pode ser modificado. Ele é reservado para novos nós de storage adicionados durante a expansão do sistema StorageGRID.



a. Para editar uma nota de armazenamento existente, clique em **Editar** e modifique a etiqueta conforme necessário.

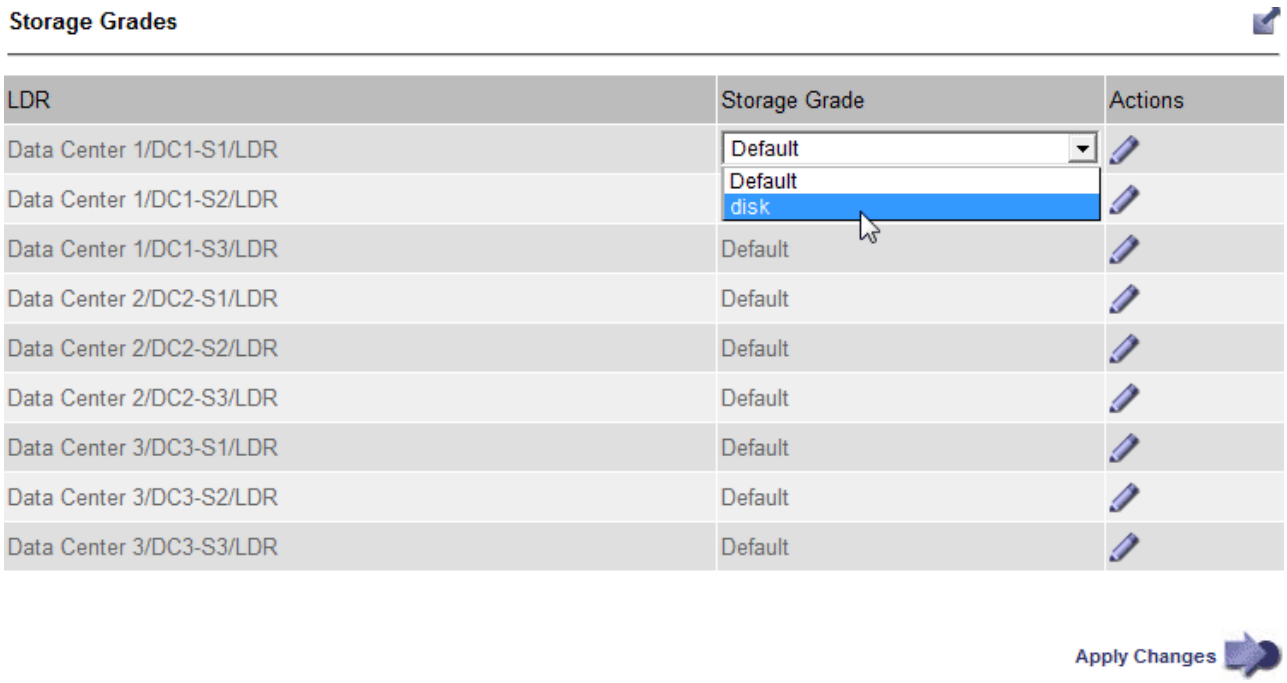
> Não é possível eliminar graus de armazenamento.

b. Clique em **aplicar alterações**.

   Esses tipos de storage agora estão disponíveis para atribuição aos nós de storage.

3. Atribuir um nível de storage a um nó de storage:

   a. Para cada serviço LDR do nó de armazenamento, clique em **Edit** e selecione uma nota de armazenamento na lista.



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.

a. Clique em **aplicar alterações**.

Configurando pools de armazenamento

Ao definir uma regra ILM, você usa pools de armazenamento para especificar onde os objetos são armazenados . Antes de criar um pool de armazenamento, você deve rever as diretrizes do pool de armazenamento.

- "O que é um pool de armazenamento"
- "Diretrizes para a criação de pools de armazenamento"
- "Uso de vários pools de storage para replicação entre locais"
- "Usando um pool de armazenamento como um local temporário (obsoleto)"
- "Criando um pool de armazenamento"
- "Visualização dos detalhes do pool de armazenamento"
- "Editando um pool de armazenamento"
- "Removendo um pool de armazenamento"

O que é um pool de armazenamento

Um pool de storage é um agrupamento lógico de nós de storage ou nós de arquivamento. Você configura pools de storage para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de storage usado.

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. 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 inclua nós de storage.

Diretrizes para a criação de pools de armazenamento

Ao configurar e usar pools de armazenamento, siga estas diretrizes.

Diretrizes para todos os pools de armazenamento

- O StorageGRID inclui um pool de storage padrão, todos os nós de storage, que usa o local padrão, todos os locais e o nível de storage padrão, todos os nós de storage. O pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adicionar novos sites de data center.

> ⓘ O uso do pool de storage todos os nós de storage ou do site todos os sites não é recomendado porque esses itens são atualizados automaticamente para incluir novos sites adicionados em uma expansão, o que pode não ser o comportamento desejado. Antes de usar o pool de storage de todos os nós de storage ou o local padrão, revise cuidadosamente as diretrizes para cópias replicadas e codificadas para apagamento.

- 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.

Diretrizes para pools de storage usados para cópias replicadas

- Crie um pool de armazenamento diferente para cada site. Em seguida, especifique um ou mais pools de armazenamento específicos do local nas instruções de posicionamento para cada regra. 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 para o novo site. Em seguida, atualize as regras do ILM para controlar quais objetos são armazenados no novo site.
- Em geral, não use o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites.

Diretrizes para pools de storage usados para cópias codificadas por apagamento

- Você não pode usar nós de arquivamento para dados codificados por apagamento.
- O número de nós de storage e sites contidos no pool de storage determina quais esquemas de codificação de apagamento estão disponíveis.

- 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.
- Em geral, não use o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites em qualquer perfil de codificação de apagamento.

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

- Se você tiver altos requisitos de taxa de transferência, não é recomendável criar um pool de armazenamento que inclua vários locais se a latência de rede entre locais for superior a 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 strict ou balanced 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).
- 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.

Diretrizes para pools de storage usados para cópias arquivadas

- 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 inclui 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. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"O que é replicação"

"O que é codificação de apagamento"

"Quais são os esquemas de codificação de apagamento"

"Uso de vários pools de storage para replicação entre locais"

"Usando um pool de armazenamento como um local temporário (obsoleto)"

"Gerenciando objetos com o S3 Object Lock"

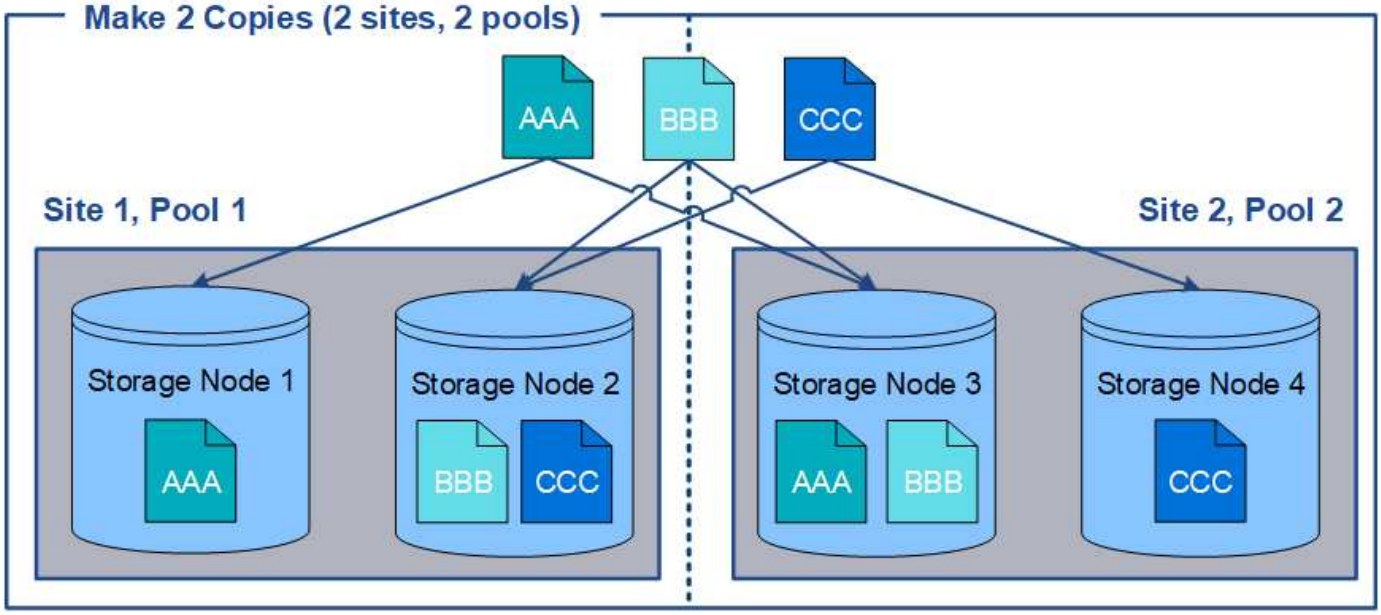
"Administrar o StorageGRID"

Uso de vários pools de storage para replicação entre locais

Se a implantação do StorageGRID incluir mais de um local, você poderá habilitar a proteção contra perda de site criando um pool de armazenamento para cada local e especificando ambos os pools de armazenamento nas instruções de posicionamento da regra. Por exemplo, se você configurar uma regra ILM para fazer duas cópias replicadas e especificar pools de armazenamento em dois locais, uma cópia de cada objeto será colocada em cada local. Se você configurar uma regra para fazer duas cópias e especificar três pools de storage, as cópias serão distribuídas para equilibrar o uso do disco entre os pools de storage, ao mesmo tempo em que garante que as duas cópias sejam armazenadas em locais diferentes.

O exemplo a seguir ilustra o que pode acontecer se uma regra ILM colocar cópias de objetos replicadas em um único pool de storage que contém nós de storage de dois locais. Como o sistema usa todos os nós disponíveis no pool de storage quando ele coloca as cópias replicadas, ele pode colocar todas as cópias de alguns objetos em apenas um dos sites. Neste exemplo, o sistema armazenou duas cópias do objeto AAA em nós de armazenamento no local 1 e duas cópias do objeto CCC em nós de armazenamento no local 2. Somente o objeto BBB é protegido se um dos sites falhar ou se tornar inacessível.

Em contraste, este exemplo ilustra como os objetos são armazenados quando você usa vários pools de armazenamento. No exemplo, a regra ILM especifica que duas cópias replicadas de cada objeto serão criadas e que as cópias serão distribuídas em dois pools de storage. Cada pool de storage contém todos os nós de storage em um local. Como uma cópia de cada objeto é armazenada em cada site, os dados do objeto são protegidos contra falha ou inacessibilidade do site.



Ao usar vários pools de armazenamento, tenha em mente as seguintes regras:

- Se você estiver criando n cópias, será necessário adicionar n ou mais pools de armazenamento. Por exemplo, se uma regra estiver configurada para fazer três cópias, especifique três ou mais pools de storage.

- 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, o sistema distribui as cópias para manter o uso do disco entre os pools balanceado e garantir que duas ou mais cópias não sejam armazenadas no mesmo pool de storage.
- 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.

Usando um pool de armazenamento como um local temporário (obsoleto)

Quando você cria uma regra ILM com um posicionamento de objeto que inclui um único pool de armazenamento, você será solicitado a especificar um segundo pool de armazenamento para usar como um local temporário.

Os locais temporários foram obsoletos e serão removidos em uma versão futura. Você não deve selecionar um pool de armazenamento como um local temporário para uma nova regra ILM.

> Se você selecionar o comportamento de ingestão estrita (Etapa 3 do assistente criar regra ILM), o local temporário será ignorado.

Informações relacionadas

"Opções de proteção de dados para ingestão"

Criando 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter revisado 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. Selecione o ícone de mais ➕para adicionar uma entrada para cada site.

Não inclua o local padrão de 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 passoConsulte 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.

  "Diretrizes para a criação de pools de armazenamento"

Passos

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

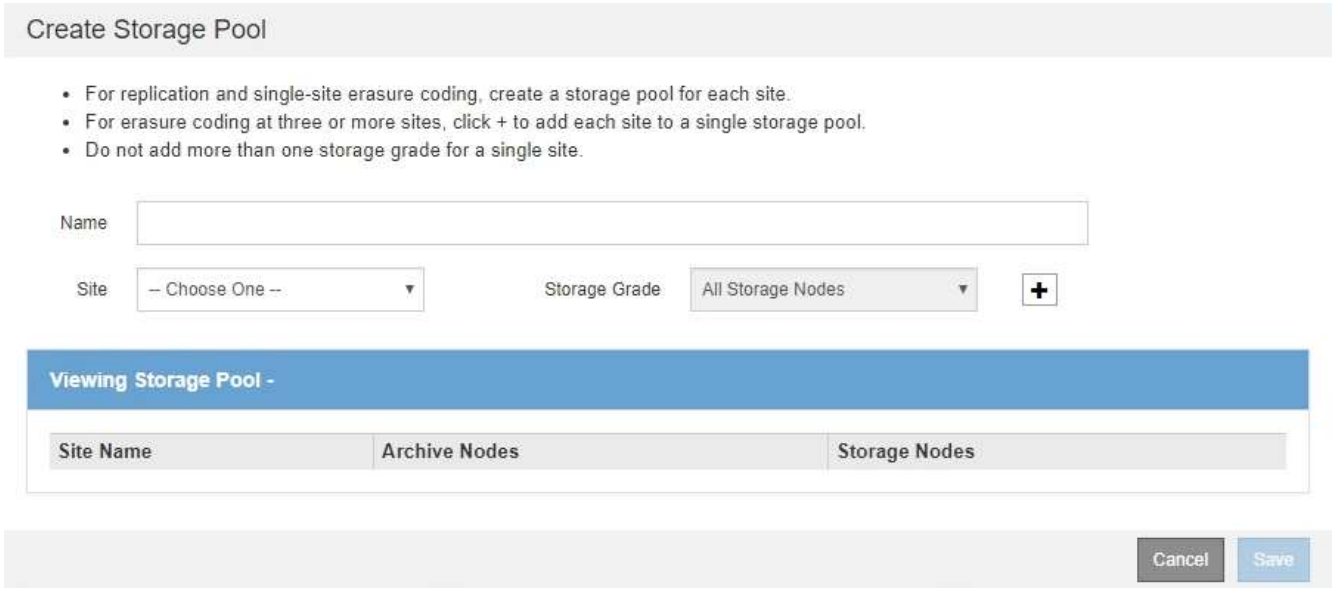
   A página pools de armazenamento é exibida e lista todos os pools de armazenamento definidos.

   A lista inclui o pool de storage padrão do sistema, todos os nós de storage, que usa o site padrão do sistema, todos os sites e a categoria de storage padrão, todos os nós de storage.

   Como o pool de storage de todos os nós de storage é atualizado automaticamente sempre que você adiciona novos locais de data center, o uso desse pool de storage em regras de ILM não é recomendado.

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

   A caixa de diálogo criar pool de armazenamento é exibida.



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.

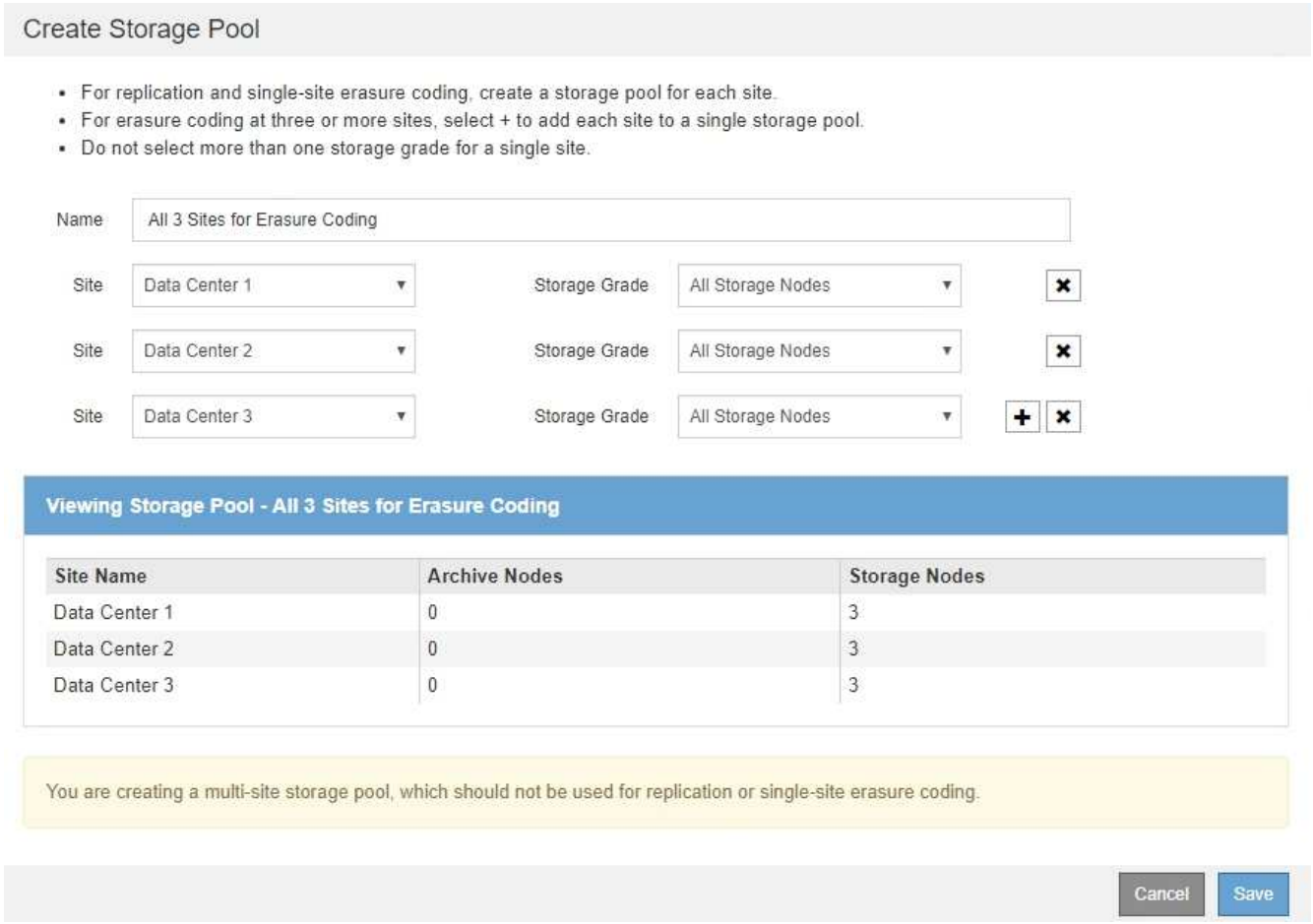
4. Na lista suspensa **Site**, selecione um site para esse pool de armazenamento.

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

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 padrão de todos os nós 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 para adicionar uma entrada para cada site ao pool de armazenamento.



É impedido de criar entradas duplicadas ou de criar um pool de armazenamento que inclua o grau de armazenamento **Archive Nodes** e qualquer tipo de armazenamento que contenha nós de armazenamento.

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

Para remover uma entrada, ✖selecione .

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

   O novo pool de armazenamento é adicionado à lista.

Informações relacionadas

"Diretrizes para a criação de pools de armazenamento"

Visualização dos 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.

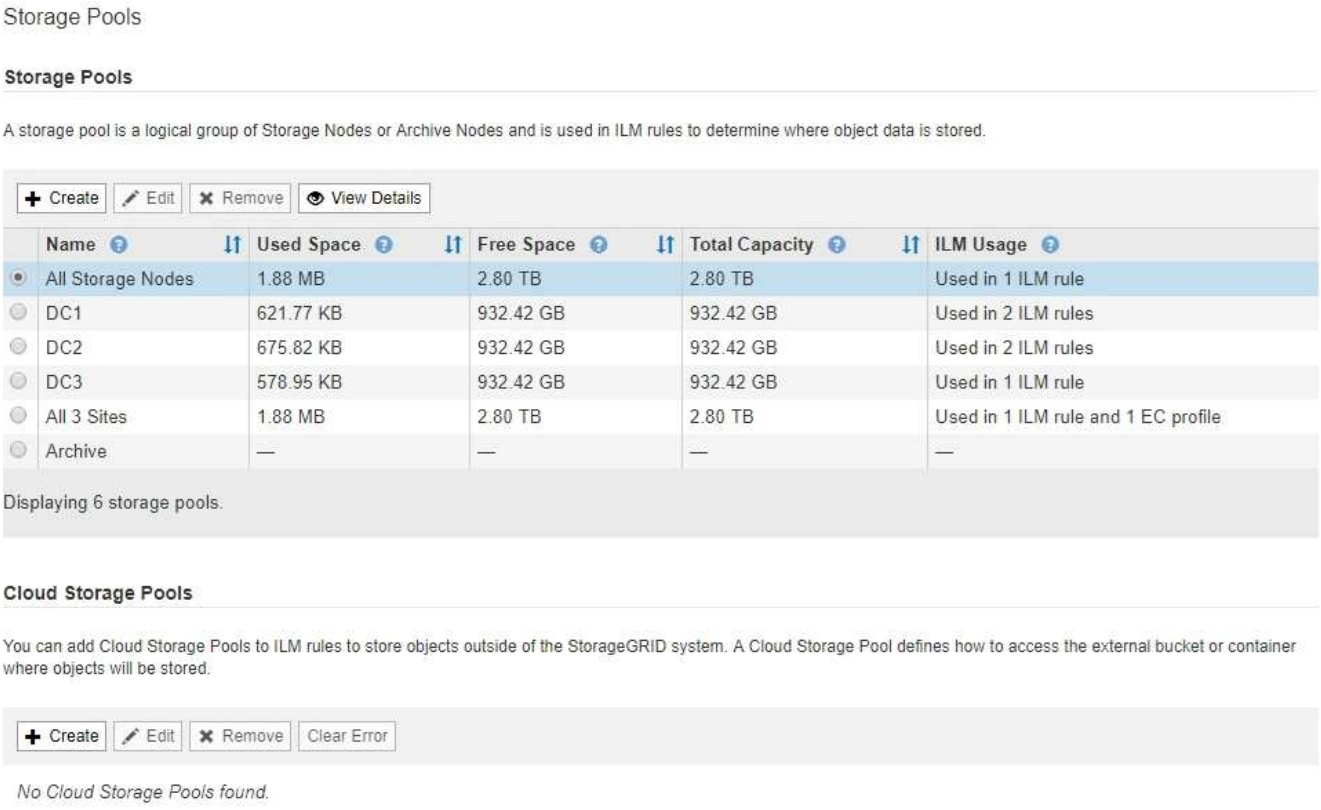
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

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

   A página conjuntos de armazenamento é exibida. Esta página lista todos os pools de armazenamento definidos.



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

   - **Nome**: O nome de exibição exclusivo do pool de armazenamento.
   - **Espaço usado**: A quantidade de espaço que está sendo usada atualmente para armazenar objetos no pool de armazenamento.
   - **Espaço livre**: A quantidade de espaço que permanece disponível para armazenar objetos no pool de armazenamento.
   - **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 do 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.

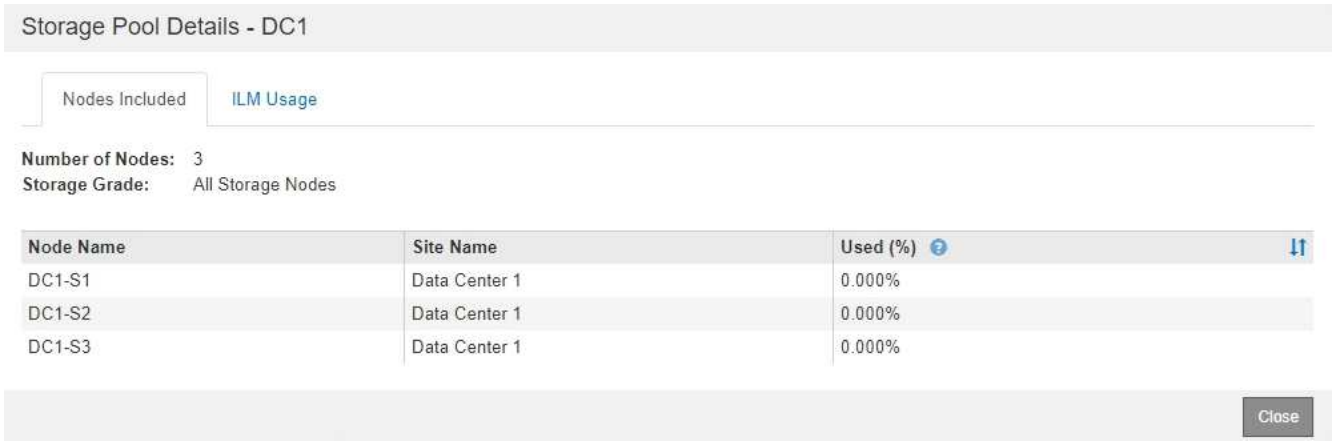
     Você não pode remover um pool de armazenamento se ele estiver sendo usado.

2. Para ver detalhes sobre um pool de armazenamento específico, selecione seu botão de opção e selecione **Exibir detalhes**.

   O modal Detalhes do conjunto de armazenamento é exibido.

3. Exiba a guia **nós incluídos** para saber mais sobre os nós de armazenamento ou nós de arquivamento

incluídos no pool de armazenamento.



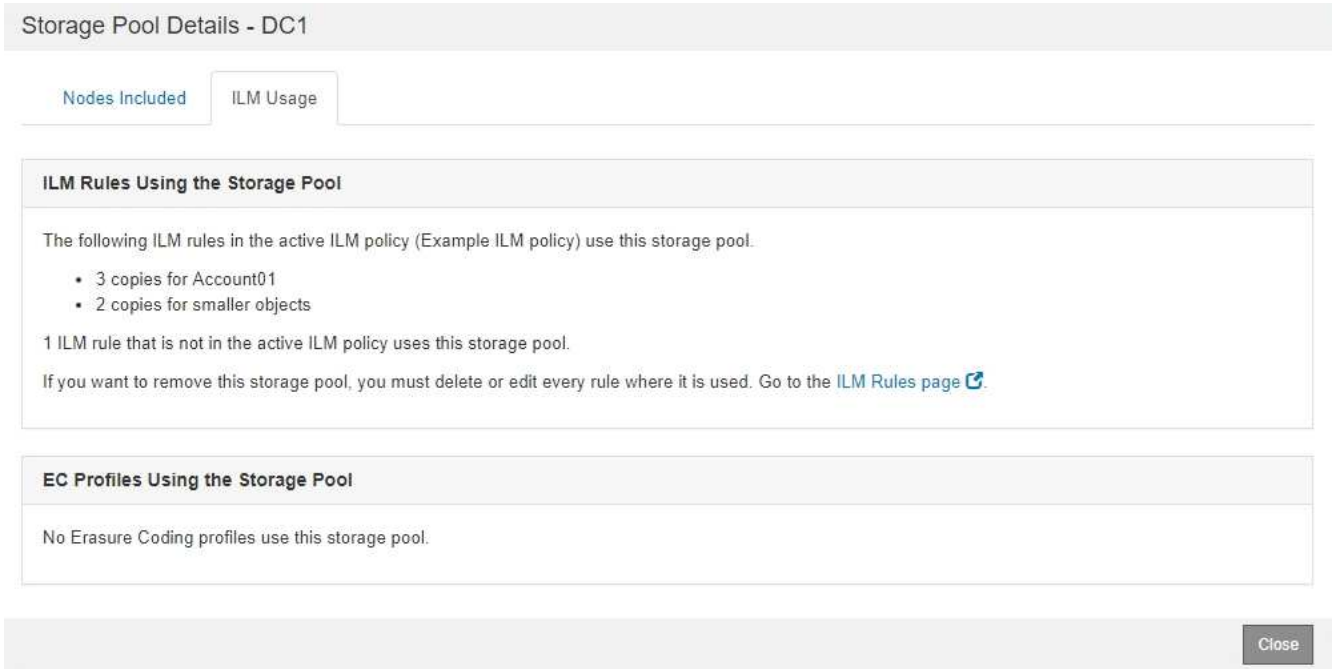
A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do local
- Usado (%): Para nós de storage, a porcentagem do espaço utilizável total para dados de objetos que foram usados. Esse valor não inclui metadados de objetos.

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

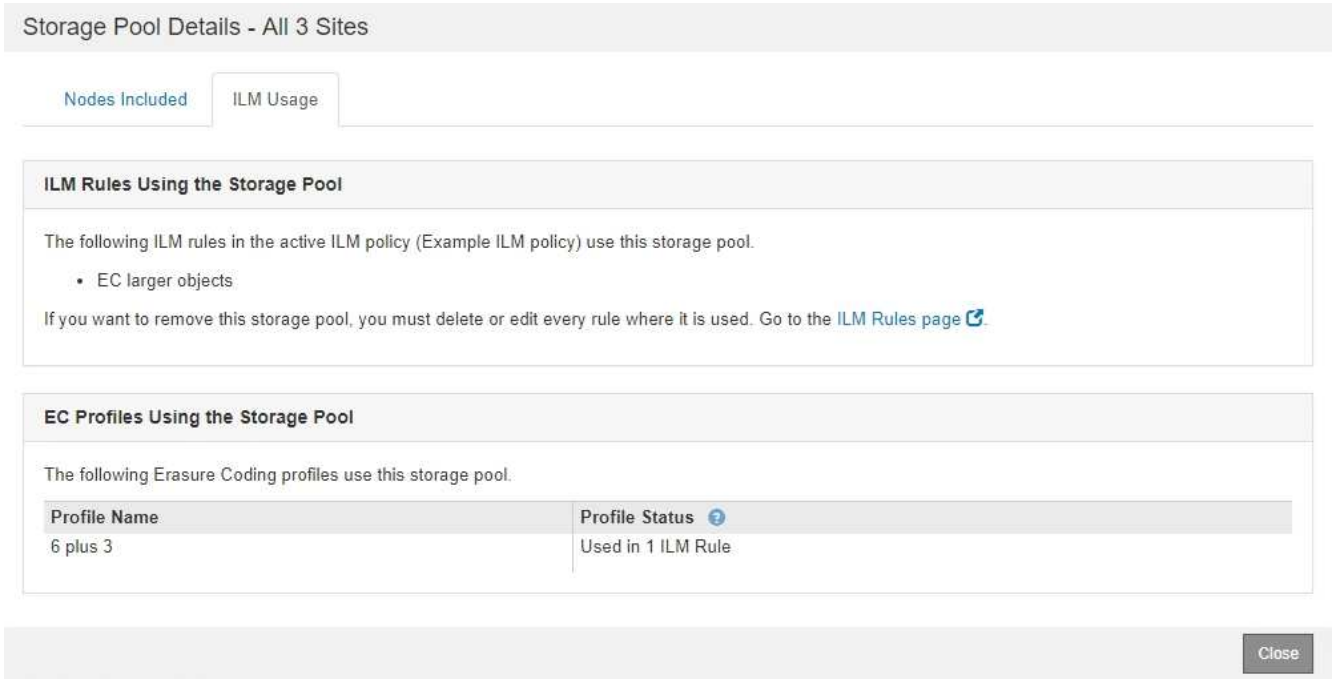
4. Selecione a guia **uso de ILM** para determinar se o pool de armazenamento está sendo usado atualmente em quaisquer regras de ILM ou perfis de codificação de apagamento.

   Neste exemplo, o pool de armazenamento DC1 é usado em três regras ILM: Duas regras que estão na política ILM ativa e uma regra que não está na política ativa.



Você não pode remover um pool de armazenamento se ele for usado em uma regra ILM.

Neste exemplo, o pool de armazenamento de todos os 3 sites é usado em um perfil de codificação de apagamento. Por sua vez, esse perfil de codificação de apagamento é usado por uma regra ILM na política ILM ativa.



Não é possível remover um pool de armazenamento se ele for usado em um perfil 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 as instruções para trabalhar com regras ILM.

6. Quando terminar de visualizar os detalhes do conjunto de armazenamento, selecione **Fechar**.

Informações relacionadas

"Trabalhando com regras de ILM e políticas de ILM"

Editando um pool de armazenamento

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter revisado as 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 deve ter considerado como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

Se você estiver adicionando um novo nível de storage a um pool de storage usado na política de ILM ativa, saiba que os nós de storage no novo nível de storage não serão usados automaticamente. Para forçar o StorageGRID a usar um novo 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**.

   A página conjuntos de armazenamento é exibida.

2. Selecione o botão de opção para o pool de armazenamento que deseja editar.

   Não é possível editar o pool de storage todos os nós de storage.

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, uma vez que a alteração tornaria o esquema de codificação de apagamento inválido.

6. Selecione **Guardar**.

Depois de terminar

Se você adicionou um novo 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 nível de armazenamento. Por exemplo, clone sua política ILM existente e, em seguida, ative o clone.

Removendo um pool de armazenamento

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

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

   A página conjuntos de armazenamento é exibida.

2. Observe a coluna 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 **Exibir detalhes** > **uso do ILM** para determinar onde um pool de armazenamento é usado.

3. Se o conjunto de armazenamento que pretende remover não estiver a ser utilizado, selecione o botão de opção.
4. Selecione **Remover**.
5. Selecione **OK**.

Usando Cloud Storage Pools

Você pode usar o Cloud Storage Pools para mover objetos do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Mover objetos para fora da grade permite que você aproveite uma camada de storage de baixo custo para arquivamento de longo prazo.

- "O que é um Cloud Storage Pool"
- "Ciclo de vida de um objeto Cloud Storage Pool"
- "Quando usar Cloud Storage Pools"
- "Considerações para pools de storage em nuvem"
- "Comparação do Cloud Storage Pools e da replicação do CloudMirror"
- "Criando um pool de armazenamento em nuvem"
- "Editando um pool de armazenamento em nuvem"
- "Removendo um pool de armazenamento em nuvem"
- "Solução de problemas de 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, é possível mover objetos acessados com pouca frequência para storage de nuvem de baixo custo, como Amazon S3 Glacier, S3 Glacier Deep Archive ou a camada de acesso de arquivamento no storage Microsoft Azure Blob. 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).

A tabela a seguir 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. Você deve configurar classes de armazenamento antes de criar o pool de armazenamento.	Usando a opção **ILM** > **Storage Pools** no Gerenciador de Grade. 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.
Onde os objetos são armazenados?	Em um ou mais nós de storage ou nós de arquivamento no StorageGRID.	Em um bucket do Amazon S3 ou contêiner de storage Azure Blob externo ao sistema StorageGRID. Se o Cloud Storage Pool for um bucket do Amazon S3: • 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. Se o pool de storage de nuvem for um contêiner de storage de Blob do Azure, o StorageGRID fará o transição do objeto para a categoria Archive. **Observação:** em geral, não configure o gerenciamento do ciclo de vida do armazenamento de Blobs do Azure para o contêiner usado em um pool de storage de nuvem. As operações de restauração PÓS-objeto em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.
O que controla o posicionamento do objeto?	Uma regra ILM na política ILM ativa.	Uma regra ILM na política ILM ativa.

	Pool de storage	Cloud Storage Pool
Que método de proteção de dados é usado?	Replicação ou codificação de apagamento.	Replicação.
Quantas cópias de cada objeto são permitidas?	Vários.	Uma cópia no pool de storage de nuvem e, opcionalmente, uma ou mais cópias no StorageGRID. **Observação:** você não pode armazenar um objeto em mais de um pool de armazenamento em nuvem a qualquer momento.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo.

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.

Informações relacionadas

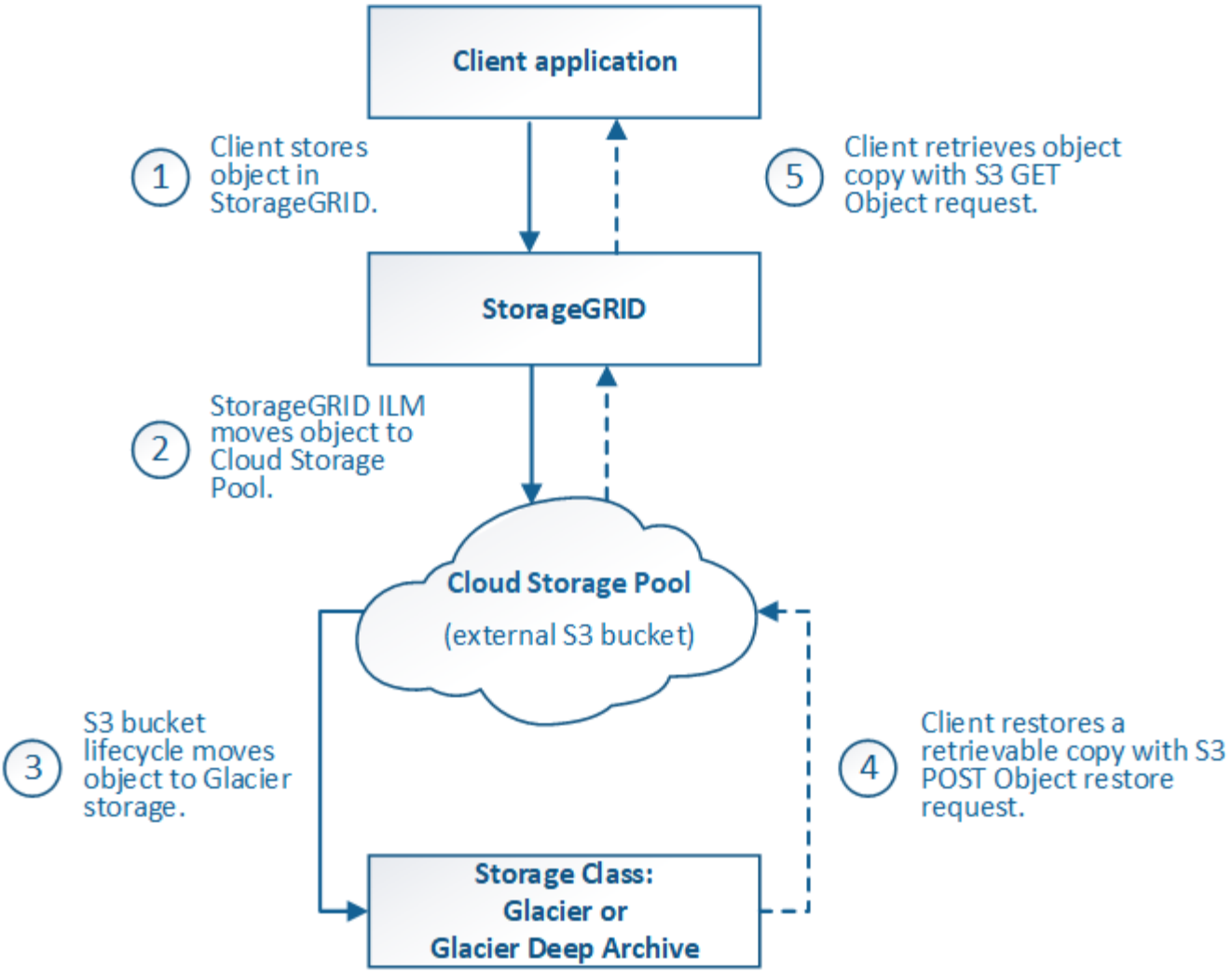
S3: Ciclo de vida de um objeto Cloud Storage Pool

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.



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**

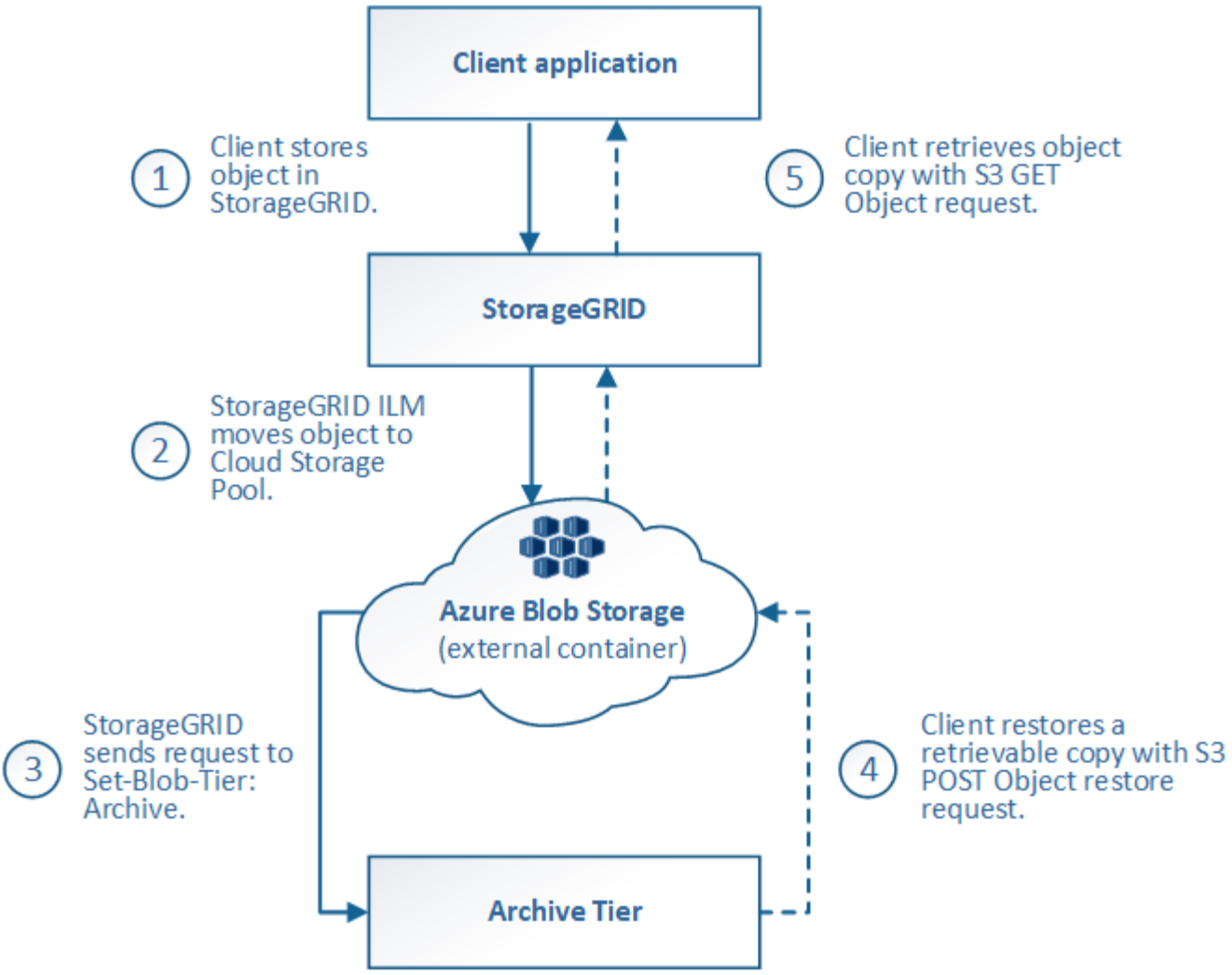
   Uma vez que um objeto foi restaurado, o aplicativo cliente pode emitir uma solicitação GET Object para recuperar o objeto restaurado.

Informações relacionadas

"Use S3"

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.

Quando usar Cloud Storage Pools

Os pools de storage em nuvem podem fornecer benefícios significativos em vários casos de uso.

Fazer backup de dados 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.

Disposição em camadas de dados do StorageGRID para um 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 pools de storage em nuvem 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 armazenamento do Blob do Azure. Ou, talvez você queira mover dados entre o Amazon S3 Glacier e o storage Azure Blob. Ao usar vários pools de armazenamento em nuvem, 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.

Informações necessárias para criar um pool de armazenamento em nuvem

Antes de criar um Cloud Storage Pool, você precisa criar o bucket externo do S3 ou o contêiner de storage externo de Blob do Azure que usará no Cloud Storage Pool. Em seguida, ao criar o pool de armazenamento em nuvem no StorageGRID, você deve especificar as seguintes informações:

- O tipo de provedor: Armazenamento Amazon S3 ou Azure Blob.
- Se você selecionar Amazon S3, se o pool de armazenamento em nuvem é para uso com a região secreta da AWS (**CAP (C2S Access Portal)**).
- O nome exato do balde ou recipiente.
- O endpoint de serviço necessário para acessar o bucket ou o contentor.
- A autenticação necessária para acessar o bucket ou o contentor:
  - **S3**: Opcionalmente, uma ID de chave de acesso e chave de acesso secreta.
  - **C2S**: A URL completa para obter credenciais temporárias do SERVIDOR CAP; um certificado CA de servidor, um certificado de cliente, uma chave privada para o certificado de cliente e, se a chave privada for criptografada, a senha para descriptografá-lo.
  - **Armazenamento Blob do Azure**: Um nome de conta e chave de conta. Essas credenciais devem ter permissão completa para o contentor.
- Opcionalmente, um certificado de CA personalizado para verificar conexões TLS com o bucket ou contentor.

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 conetividade 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 coneta ao endpoint externo do pool de armazenamento em nuvem, ele emite várias solicitações para monitorar a conetividade 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. Neste caso, você simplesmente 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 de ciclo de vida do Azure Blob Storage 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

"Criando um pool de armazenamento em nuvem"

"S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

"C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

"Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

"Administrar o StorageGRID"

Comparação do Cloud Storage Pools e da 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?	Um pool de storage em nuvem atua como destino de arquivamento. 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 apenas uma cópia no StorageGRID e enviar uma cópia para o pool de storage de nuvem.	O serviço de replicação do CloudMirror permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket externo do S3 (destino). A replicação do CloudMirror cria uma cópia independente de um objeto em uma infraestrutura S3 independente.
Como é configurado?	Os pools de armazenamento em nuvem são definidos da mesma forma que os pools de armazenamento, usando o Gerenciador de Grade ou a API de Gerenciamento de Grade. Um pool de armazenamento em nuvem 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 Tenant ou a API 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?	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Camada de arquivamento de Blob do Azure	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3)
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.Objects do CloudMirror que existiam no bucket de origem antes que o bucket fosse configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.

	Cloud Storage Pool	Serviço de replicação do CloudMirror
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.
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 no 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.

Informações relacionadas

"Administrar o StorageGRID"

Criando um pool de armazenamento em nuvem

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.
- Você precisa ter revisado as diretrizes para configurar os pools de armazenamento em nuvem.
- O bucket externo ou o contêiner referenciado pelo Cloud Storage Pool deve existir.
- Você deve ter todas as informações de autenticação necessárias para acessar o bucket ou o contentor.

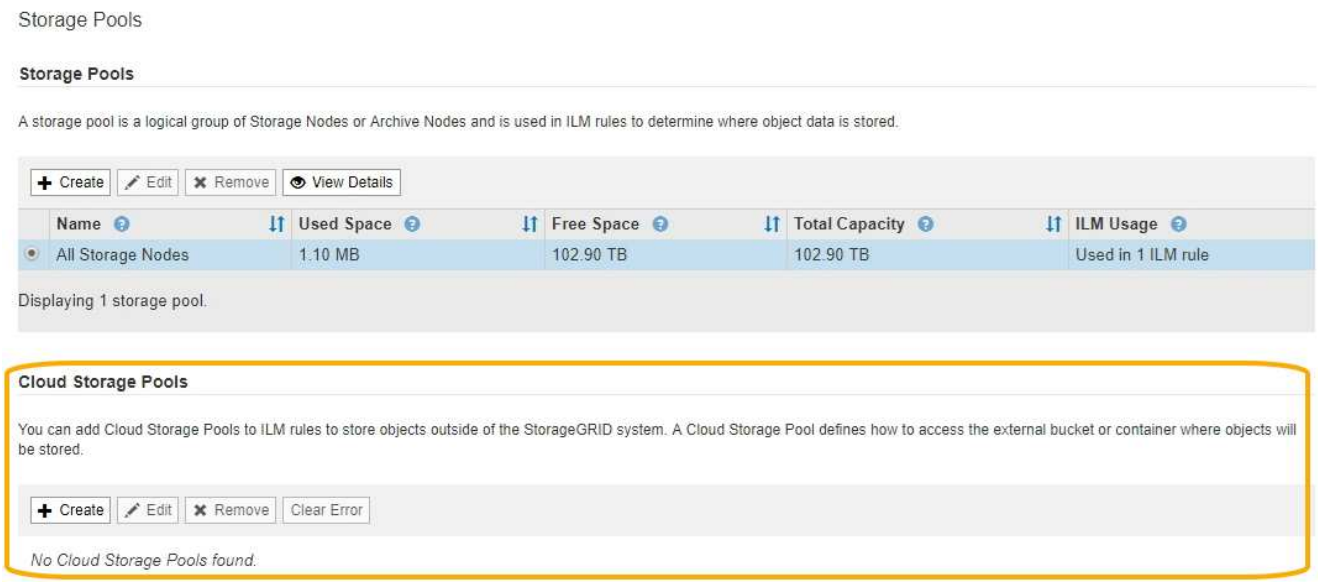
Sobre esta tarefa

Um Cloud Storage Pool especifica um único bucket externo do S3 ou contêiner de storage Azure Blob. O StorageGRID valida o pool de armazenamento em nuvem assim que você o salva, portanto, você deve garantir que o bucket ou o contentor especificado no pool de armazenamento em nuvem existe e está acessível.

Passos

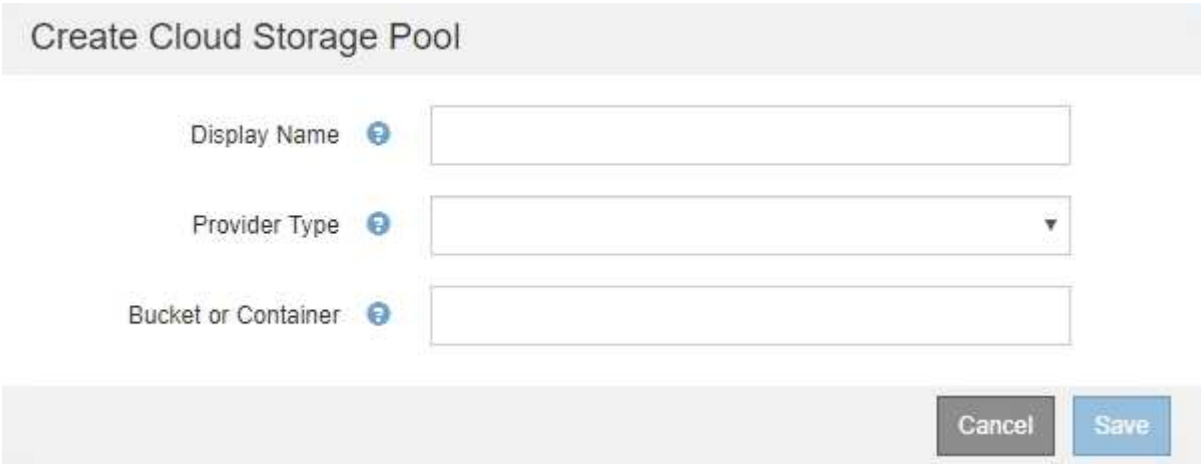
1. Selecione **ILM** > **Storage Pools**.

   A página conjuntos de armazenamento é exibida. Esta página inclui duas seções: Pools de armazenamento e pools de armazenamento em nuvem.



2. Na seção Cloud Storage Pools da página, clique em **criar**.

   A caixa de diálogo criar pool de armazenamento em nuvem é exibida.



3. Introduza as seguintes informações:

Campo	Descrição
Nome de exibição	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.
Tipo de fornecedor	Qual provedor de nuvem você usará para este pool de armazenamento em nuvem: • Amazon S3 (selecione essa opção para um pool de armazenamento em nuvem S3 ou C2S S3) • Storage Blob do Azure **Observação:** quando você seleciona um tipo de provedor, as seções ponto final do serviço, Autenticação e Verificação do servidor aparecem na parte inferior da página.
Balde ou recipiente	O nome do bucket externo do S3 ou do contêiner do Azure que foi criado para o Cloud Storage Pool. O nome especificado aqui deve corresponder exatamente ao nome do bucket ou do contentor ou a criação do Cloud Storage Pool falhará. Você não pode alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

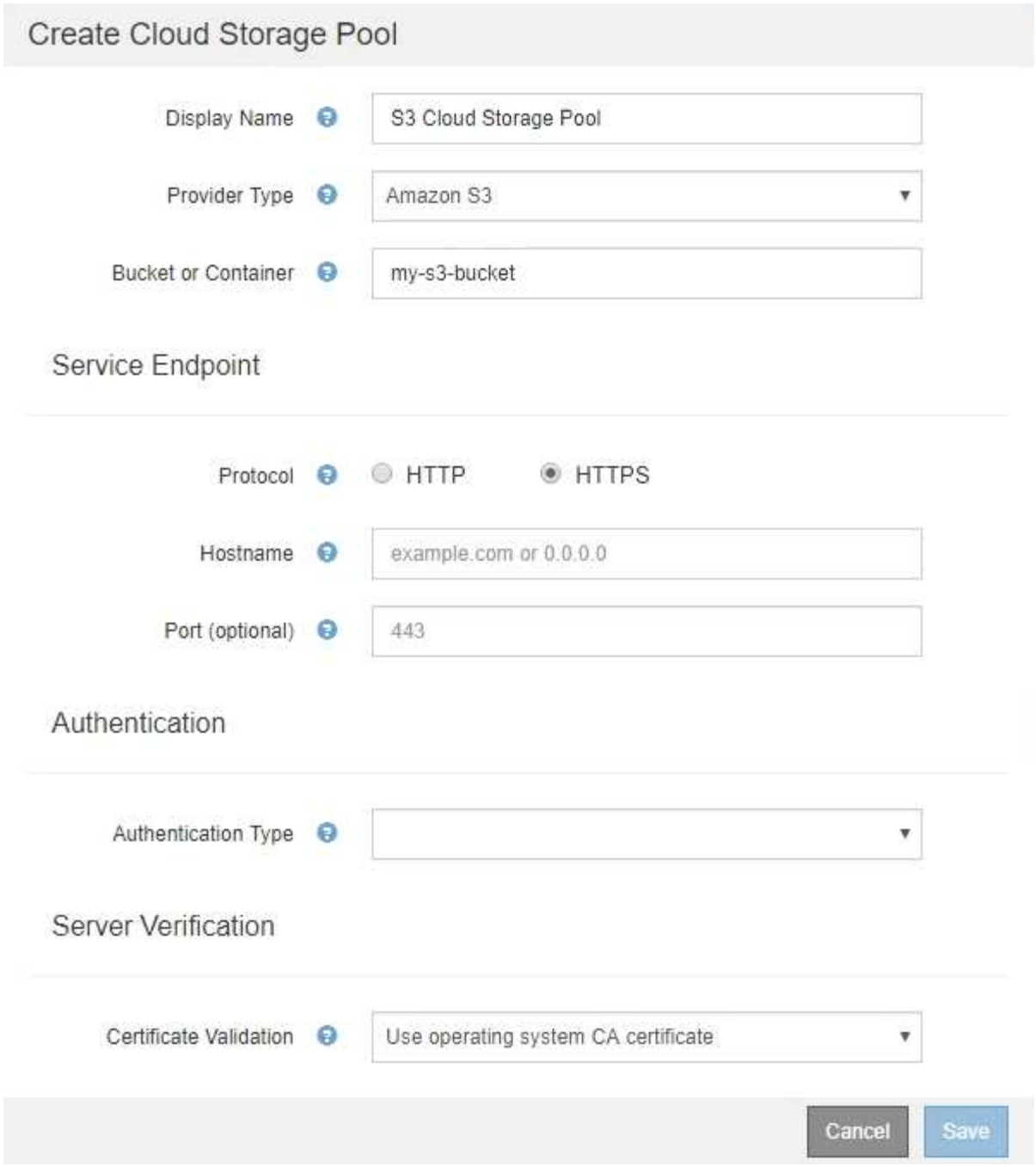
4. Preencha as seções Service Endpoint, Authentication e Server Verification da página, com base no tipo de provedor selecionado.
   - "S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"
   - "C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"
   - "Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem"

S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Ao criar um pool de armazenamento em nuvem para S3, você deve selecionar o tipo de autenticação necessário para o ponto de extremidade do pool de armazenamento em nuvem. Você pode especificar anônimo ou inserir um ID de chave de acesso e chave de acesso secreta.

O que você vai precisar

- Você deve ter inserido as informações básicas do Cloud Storage Pool e especificado **Amazon S3** como o tipo de provedor.



- Se você estiver usando a autenticação da chave de acesso, você deve saber o ID da chave de acesso e a chave de acesso secreta para o bucket externo do S3.

Passos

1. Na seção **Service Endpoint**, forneça as seguintes informações:

   a. Selecione qual protocolo usar ao se conetar ao pool de armazenamento em nuvem.

      O protocolo padrão é HTTPS.

   b. Insira o nome do host do servidor ou o endereço IP do pool de armazenamento em nuvem.

      Por exemplo:

`s3-aws-region.amazonaws.com`

> Não inclua o nome do intervalo neste campo. Você inclui o nome do bucket no campo **Bucket ou Container**.

a. Opcionalmente, especifique a porta que deve ser usada ao se conetar ao Cloud Storage Pool.

   Deixe este campo em branco para usar a porta padrão: Porta 443 para HTTPS ou porta 80 para HTTP.

2. Na seção **Autenticação**, selecione o tipo de autenticação necessário para o endpoint Cloud Storage Pool.

Opção	Descrição
Chave de acesso	Um ID de chave de acesso e chave de acesso secreta são necessários para acessar o intervalo do pool de armazenamento em nuvem.
Anônimo	Todos têm acesso ao bucket do Cloud Storage Pool. Não é necessário um ID de chave de acesso e uma chave de acesso secreta.
CAP (Portal de Acesso C2S)	Usado apenas para C2S S3. Vá para "C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem".

3. Se tiver selecionado a chave de acesso, introduza as seguintes informações:

Opção	Descrição
ID da chave de acesso	O ID da chave de acesso para a conta que possui o intervalo externo.
Chave de Acesso secreta	A chave de acesso secreto associada.

4. Na seção Verificação do servidor, selecione qual método deve ser usado para validar o certificado para conexões TLS com o pool de armazenamento em nuvem:

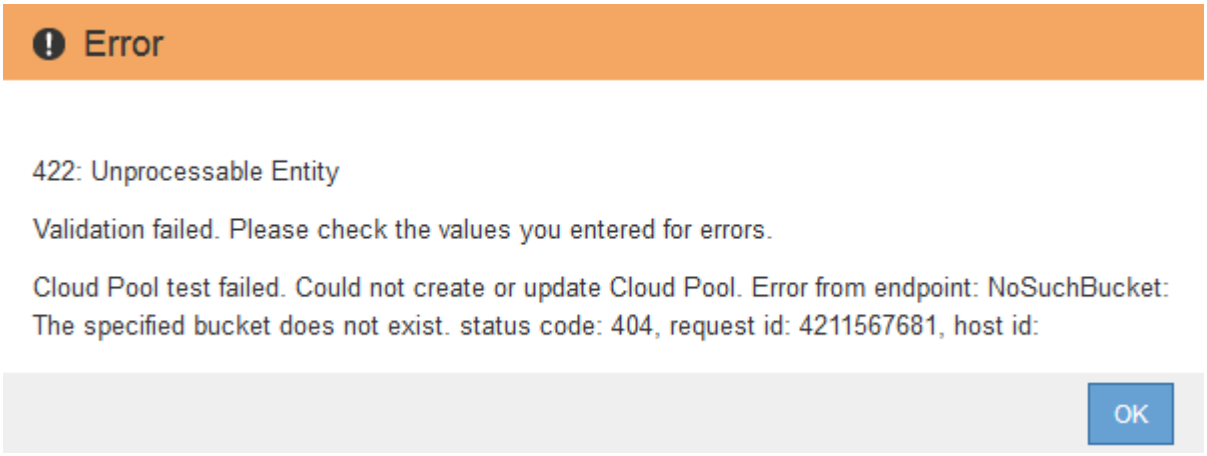
Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados de CA padrão instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Clique em **Select New** (Selecionar novo) e carregue o certificado CA codificado em PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

5. Clique em **Salvar**.

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

- Valida que o intervalo 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 para identificar o bucket como um Cloud Storage Pool. 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 intervalo especificado ainda não existir.



Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Para usar o serviço de Serviços comerciais de nuvem (C2S) S3 como um pool de armazenamento em nuvem, você deve configurar o C2S Access Portal (CAP) como o tipo de autenticação, para que a StorageGRID possa solicitar credenciais temporárias para acessar o bucket do S3 na sua conta do C2S.

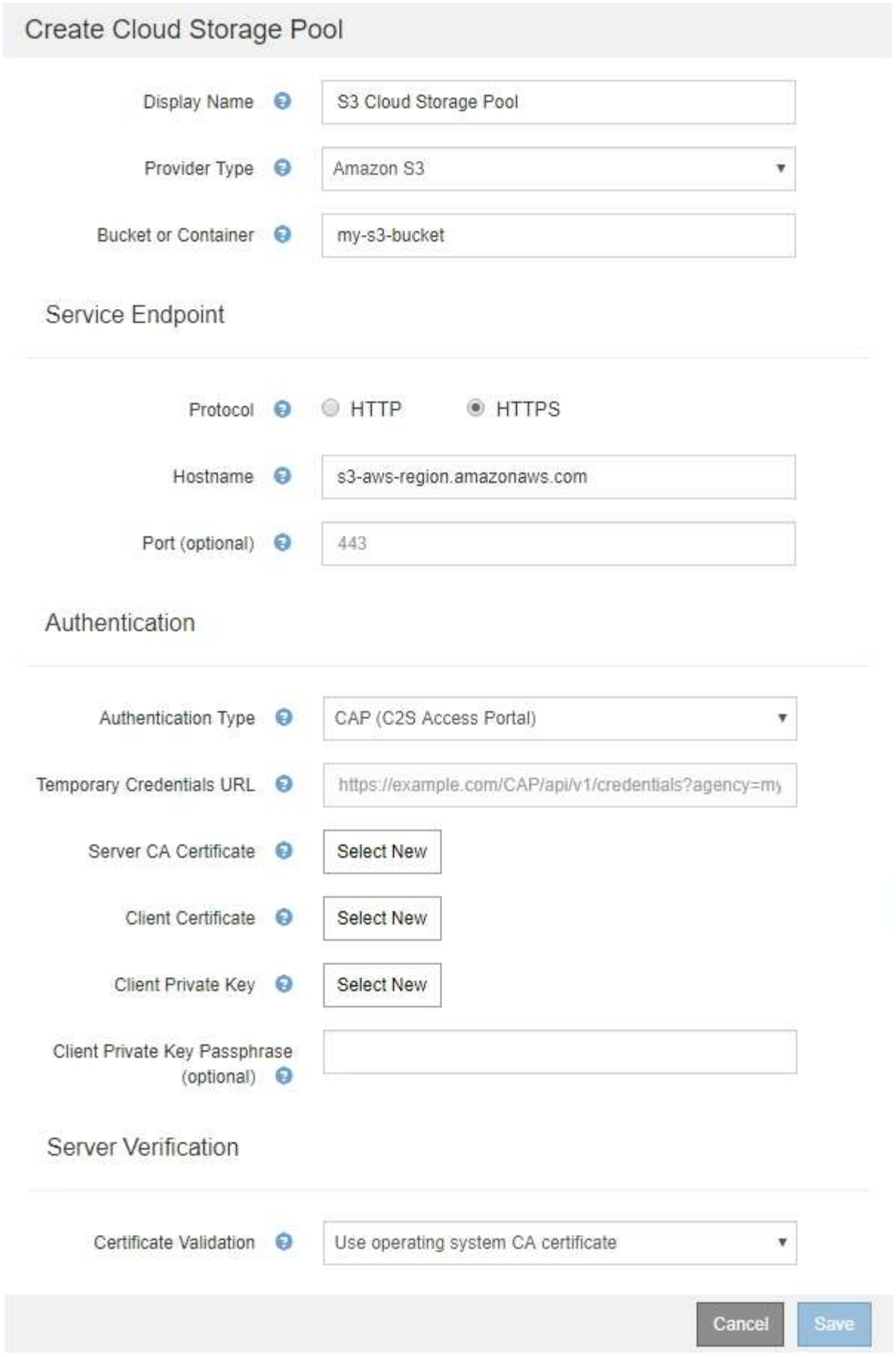
O que você vai precisar

- Você deve ter inserido as informações básicas de um pool de armazenamento em nuvem do Amazon S3, incluindo o endpoint do serviço.
- Você deve saber 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.
- Você deve ter um certificado de CA de 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.
- Você deve ter um certificado de cliente emitido por uma autoridade de certificação governamental (CA) apropriada. 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.
- Você deve ter uma chave privada codificada PEM para o certificado do cliente.
- Se a chave privada do certificado de cliente for encriptada, tem de ter a frase-passe para o desencriptar.

Passos

1. Na seção **Autenticação**, selecione **CAP (C2S Access Portal)** na lista suspensa **Authentication Type**.

   Os campos de autenticação CAP C2S aparecem.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Forneça as seguintes informações:
   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**, clique em **Selecionar novo** e carregue o certificado CA codificado em PEM que o StorageGRID usará para verificar o servidor CAP.
   c. Para **certificado de cliente**, clique em **Selecionar novo** e carregue o certificado codificado PEM que o StorageGRID usará para se identificar no servidor CAP.
   d. Para **chave privada do cliente**, clique em **Select New** e carregue a chave privada codificada pelo PEM para o certificado do cliente.

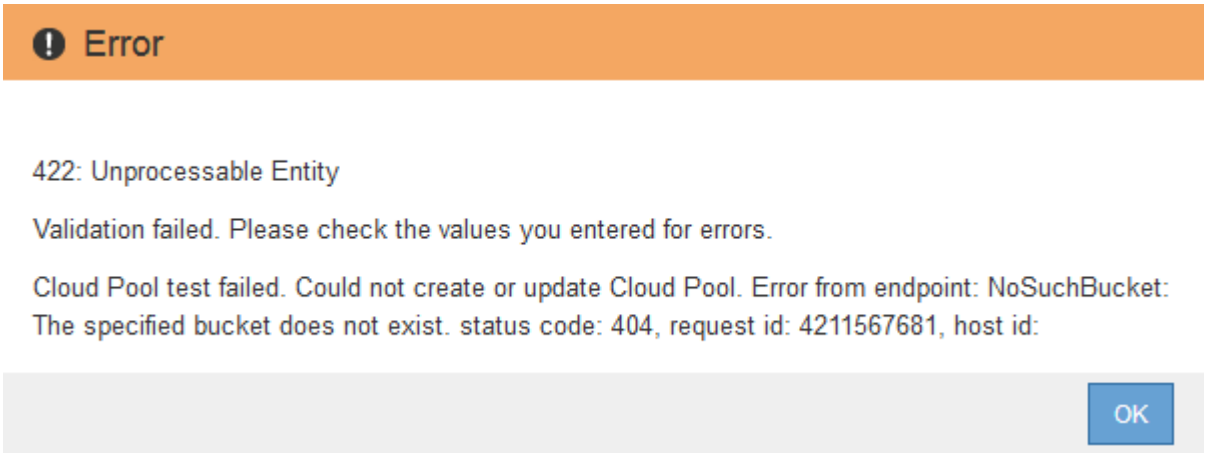
      Se a chave privada for criptografada, o formato tradicional deve ser usado. (O formato criptografado PKCS nº 8 não é suportado.)

   e. Se a chave privada do cliente estiver encriptada, introduza a frase-passe para desencriptar a chave privada do cliente. Caso contrário, deixe o campo **frase-passe de chave privada do cliente** em branco.
3. Na seção Verificação do servidor, forneça as seguintes informações:
   a. Para **Validação de certificado**, selecione **usar certificado CA personalizado**.
   b. Clique em **Select New** (Selecionar novo) e carregue o certificado CA codificado em PEM.
4. Clique em **Salvar**.

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

- Valida que o intervalo 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 para identificar o bucket como um Cloud Storage Pool. 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 intervalo especificado ainda não existir.



Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

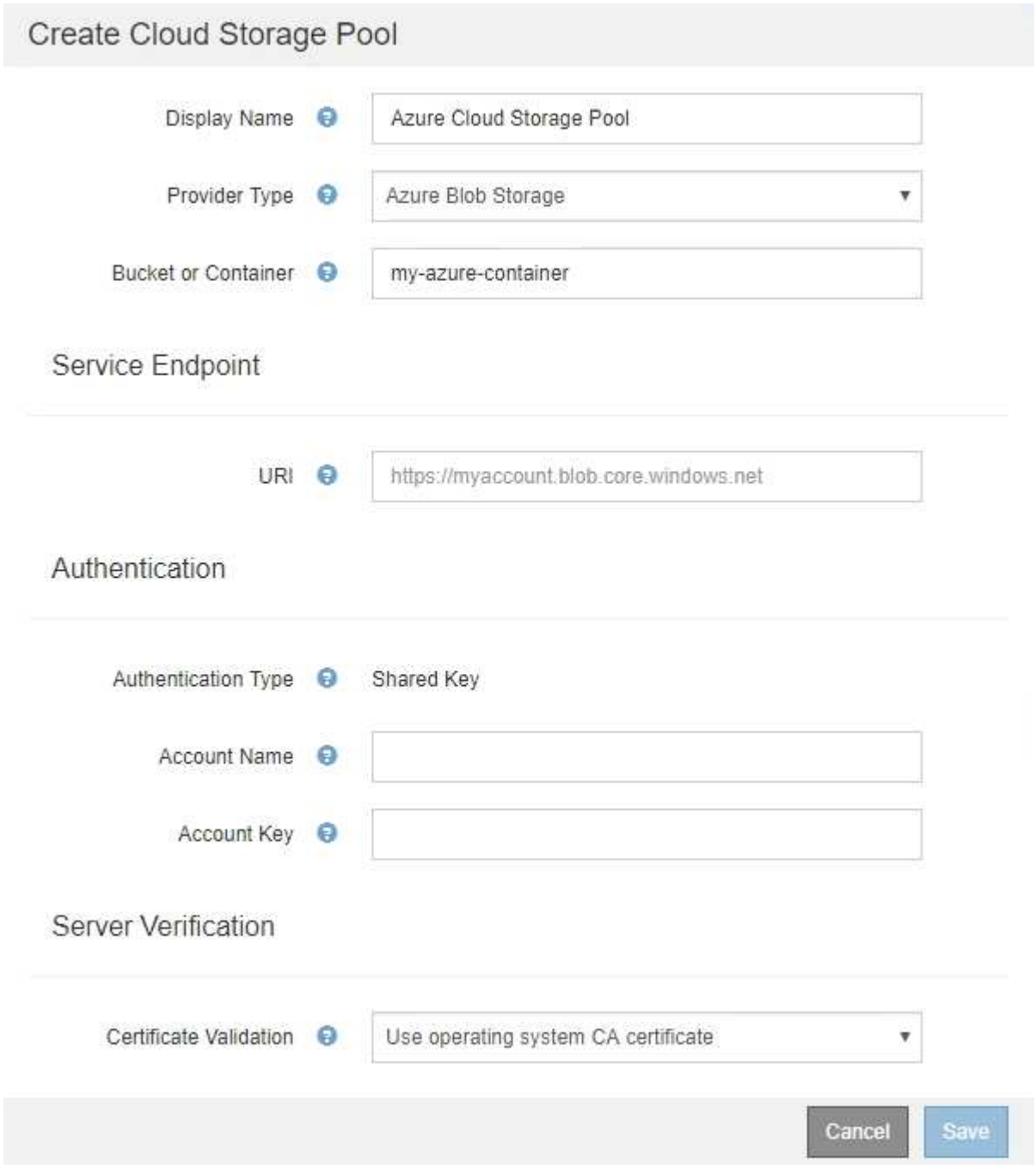
"Solução de problemas de Cloud Storage Pools"

Azure: Especificando detalhes de autenticação para um pool de armazenamento em nuvem

Ao criar um pool de storage de nuvem para storage de Blobs do Azure, você deve especificar um nome de conta e uma chave de conta para o contêiner externo que o StorageGRID usará para armazenar objetos.

O que você vai precisar

- Você precisa ter inserido as informações básicas do Cloud Storage Pool e especificado **armazenamento Blob Azure** como o tipo de provedor. **Chave compartilhada** aparece no campo **tipo de autenticação**.



- Você deve saber o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento

de Blob usado para o pool de armazenamento do Cloud Storage.

- Você deve saber o nome da conta de armazenamento e a chave secreta. Você pode usar o portal do Azure para encontrar esses valores.

Passos

1. Na seção **Service Endpoint**, insira o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento de Blob usado para o Cloud Storage Pool.

   Especifique o URI em um dos seguintes formatos:

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

   Se você não especificar uma porta, por padrão, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP. * Exemplo de URI para o contentor de armazenamento Blob do Azure* `https://myaccount.blob.core.windows.net`

2. Na seção **Autenticação**, forneça as seguintes informações:

   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.

   Para endpoints do Azure, você deve usar a autenticação chave compartilhada.

3. Na seção **Verificação do servidor**, selecione qual método deve ser usado para validar o certificado para conexões TLS ao pool de armazenamento em nuvem:

Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados de CA padrão instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Clique em **Select New** (Selecionar novo) e carregue o certificado codificado PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

4. Clique em **Salvar**.

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

- Valida que o contentor e o URI existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no contentor para identificá-lo como um Cloud Storage Pool. 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 contentor especificado ainda não existir.

Consulte as instruções para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

Editando 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.

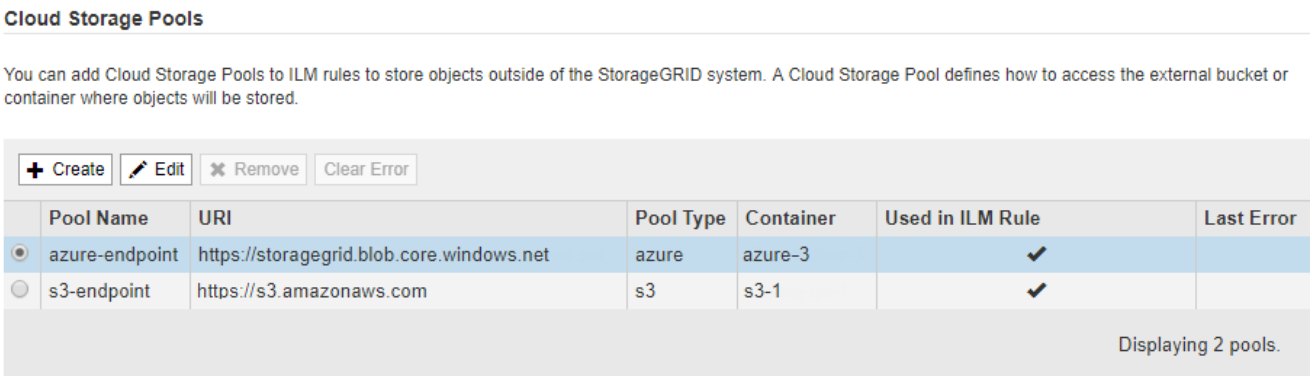
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa ter revisado as diretrizes para configurar os pools de armazenamento em nuvem.

Passos

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

   A página conjuntos de armazenamento é exibida. A tabela Cloud Storage Pools lista os pools de armazenamento em nuvem existentes.



2. Selecione o botão de opção do pool de armazenamento em nuvem que você deseja editar.
3. Clique em **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.

   > Você não pode 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 **Exibir atual** para revisar o certificado que está atualmente em uso.

5. Clique em **Salvar**.

   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 para solucionar problemas de pools de armazenamento em nuvem, resolver o problema e, em seguida, tente salvar o pool de armazenamento em nuvem novamente.

Informações relacionadas

"Considerações para pools de storage em nuvem"

"Solução de problemas de Cloud Storage Pools"

Removendo um pool de armazenamento em nuvem

Você pode remover um pool de armazenamento em nuvem que não seja usado em uma regra ILM e que não contenha dados de objeto.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- 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. Consulte ""solução de problemas de pools de armazenamento em nuvem"".

> 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 .

- Você já removeu quaisquer regras ILM que possam ter usado o pool.

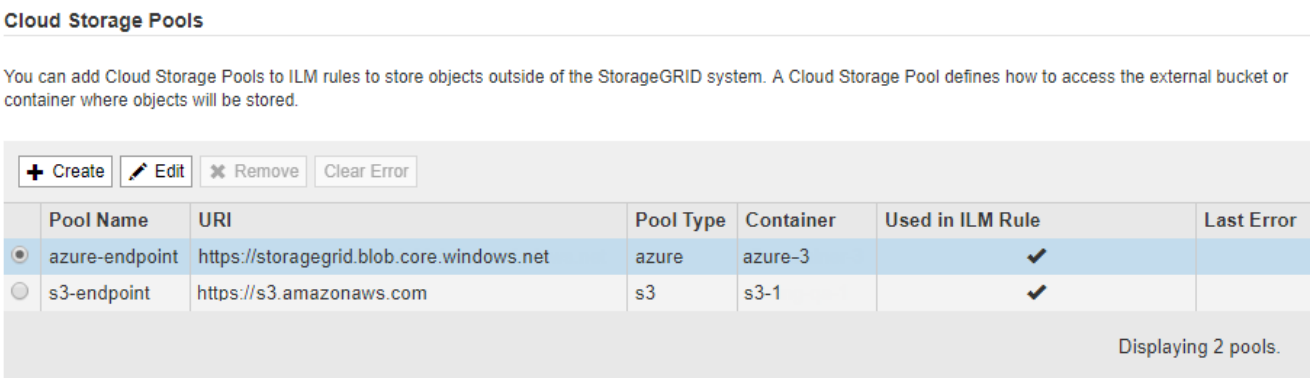
Passos

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

   A página conjuntos de armazenamento é exibida.

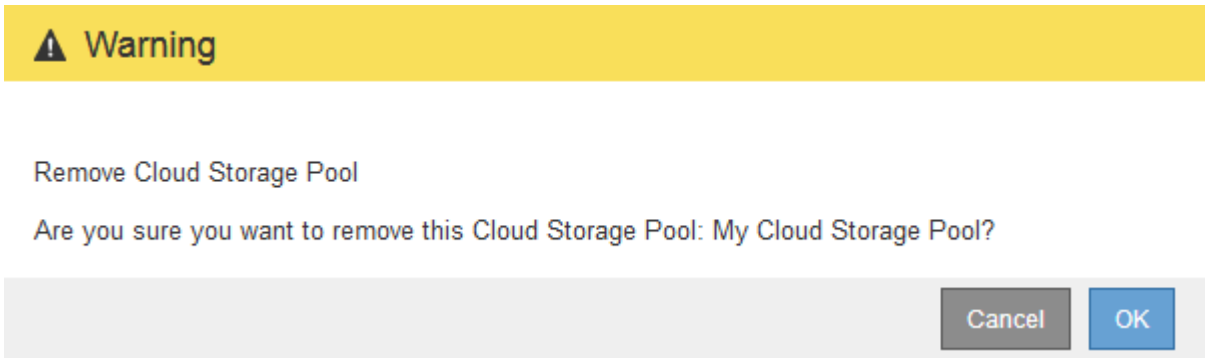
2. Selecione o botão de opção para um pool de armazenamento em nuvem que não é usado atualmente em uma regra ILM.

   Você não pode remover um pool de armazenamento em nuvem se ele for usado em uma regra ILM. O botão **Remove** está desativado.



3. Clique em **Remover**.

   É apresentado um aviso de confirmação.



4. Clique em **OK**.

   O pool de armazenamento em nuvem é removido.

Informações relacionadas

"Solução de problemas de Cloud Storage Pools"

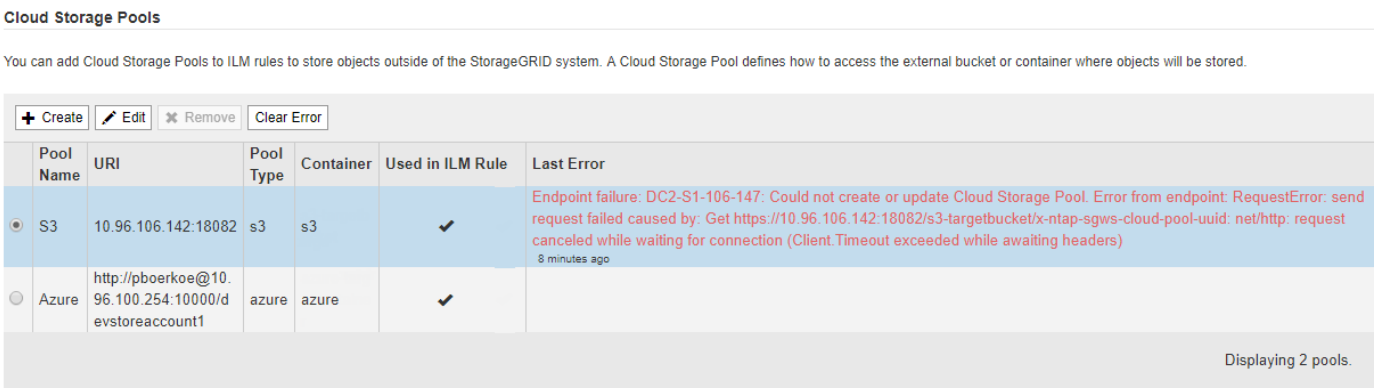
Solução de problemas de Cloud Storage Pools

Se você encontrar erros ao criar, editar ou excluir um pool de armazenamento em nuvem, siga estas etapas de solução de problemas para ajudar a resolver o problema.

Determinar 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 detetar 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 detetado para cada pool de armazenamento em nuvem e indica há quanto tempo o erro ocorreu.

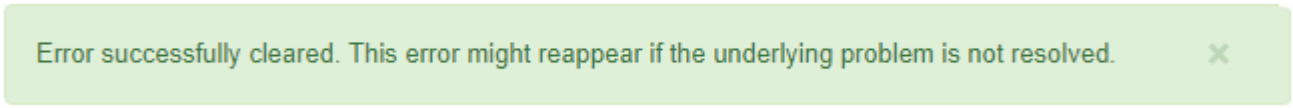


Além disso, um alerta de **erro de conetividade do Cloud Storage Pool** é acionado se a verificação de integridade detetar que um ou mais novos erros do Cloud Storage Pool ocorreram nos últimos 5 minutos. Se você receber uma notificação por e-mail para esse alerta, vá para a página conjunto de armazenamento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

as diretrizes de solução de problemas abaixo.

Verificar 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 botão de opção para o endpoint e clique em **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 tiver sido corrigido (ou se for encontrado um erro diferente), 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 conetividade 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 o protocolo 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 conetividade 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 pool de armazenamento em nuvem se ele contiver dados movidos pelo ILM, dados que estavam no bucket antes de configurar o pool de armazenamento em nuvem ou dados que foram colocados no bucket por outra fonte após a criação do pool de armazenamento em nuvem.

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 puder alcançar o endpoint 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"

Configurando perfis de codificação de apagamento

Você configura os perfis de codificação de apagamento associando um pool de storage a um esquema de codificação de apagamento, como 6-3. Em seguida, ao configurar as instruções de colocação para uma regra ILM, você pode selecionar o perfil de codificação de apagamento. Se um objeto corresponder à regra, os dados e fragmentos de paridade serão criados e distribuídos para os locais de storage no pool de storage de acordo com o esquema de codificação de apagamento.

- "Criando um perfil de codificação de apagamento"
- "Renomeando um perfil de codificação de apagamento"
- "Desativar um perfil de codificação de apagamento"

Criando um perfil de codificação de apagamento

Para criar um perfil de codificação de apagamento, você associa um pool de storage que contém nós de storage a um esquema de codificação de apagamento. Essa associação determina o número de dados e fragmentos de paridade criados e onde o sistema distribui esses fragmentos.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa criar um pool de storage que inclua exatamente um local ou um pool de storage que inclua três ou mais locais. Não há esquemas de codificação de apagamento disponíveis para um pool de storage que tenha apenas dois locais.

Sobre esta tarefa

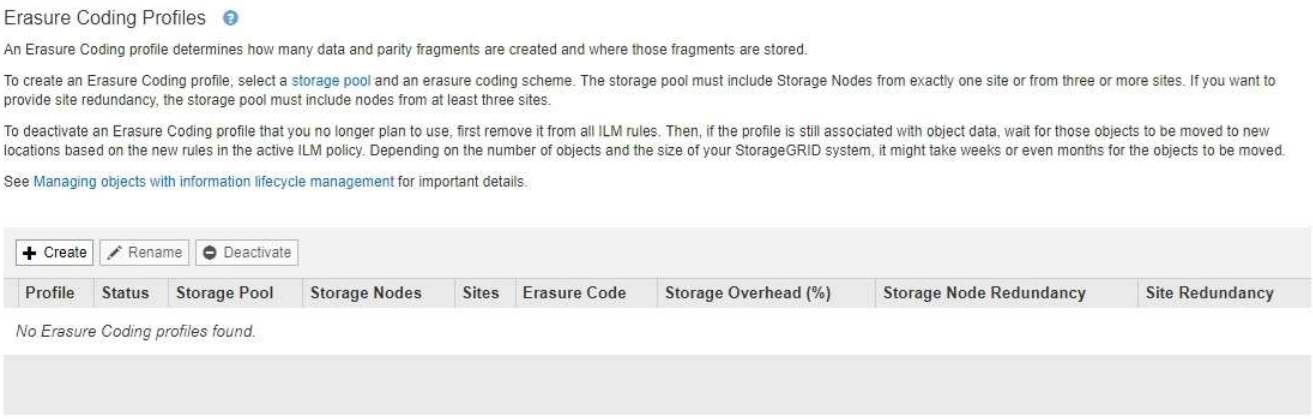
Os pools de storage usados nos perfis de codificação de apagamento devem incluir exatamente um local ou três ou mais locais. Se você quiser fornecer redundância de site, o pool de armazenamento deve ter pelo menos três locais.

> Você deve selecionar um pool de storage que contenha nós de storage. Você não pode usar nós de arquivamento para dados codificados por apagamento.

Passos

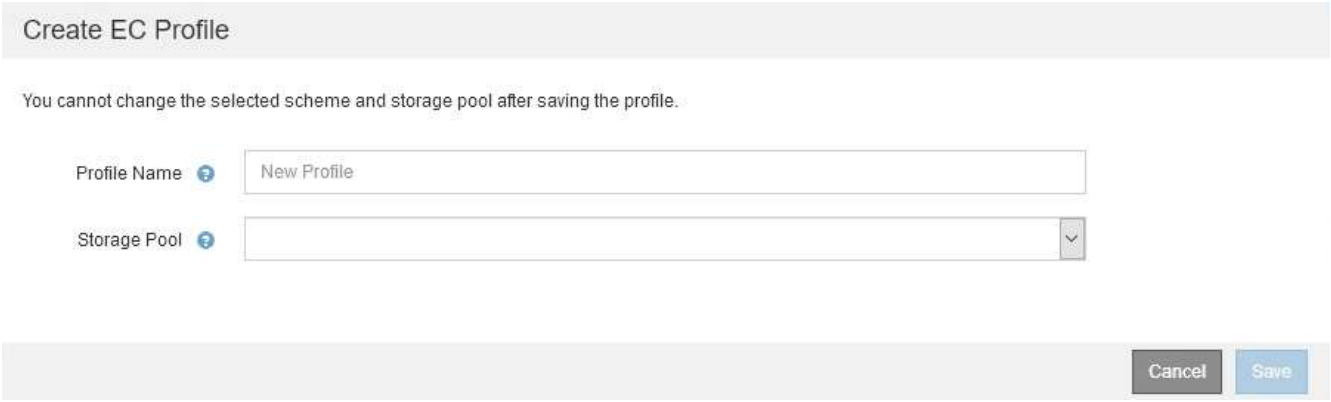
1. Selecione **ILM** > **Codificação de apagamento**.

A página Perfis de codificação de apagamento é exibida.



2. Clique em **criar**.

A caixa de diálogo criar perfil EC é exibida.



3. Introduza um nome exclusivo para o perfil de codificação de apagamento.

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.

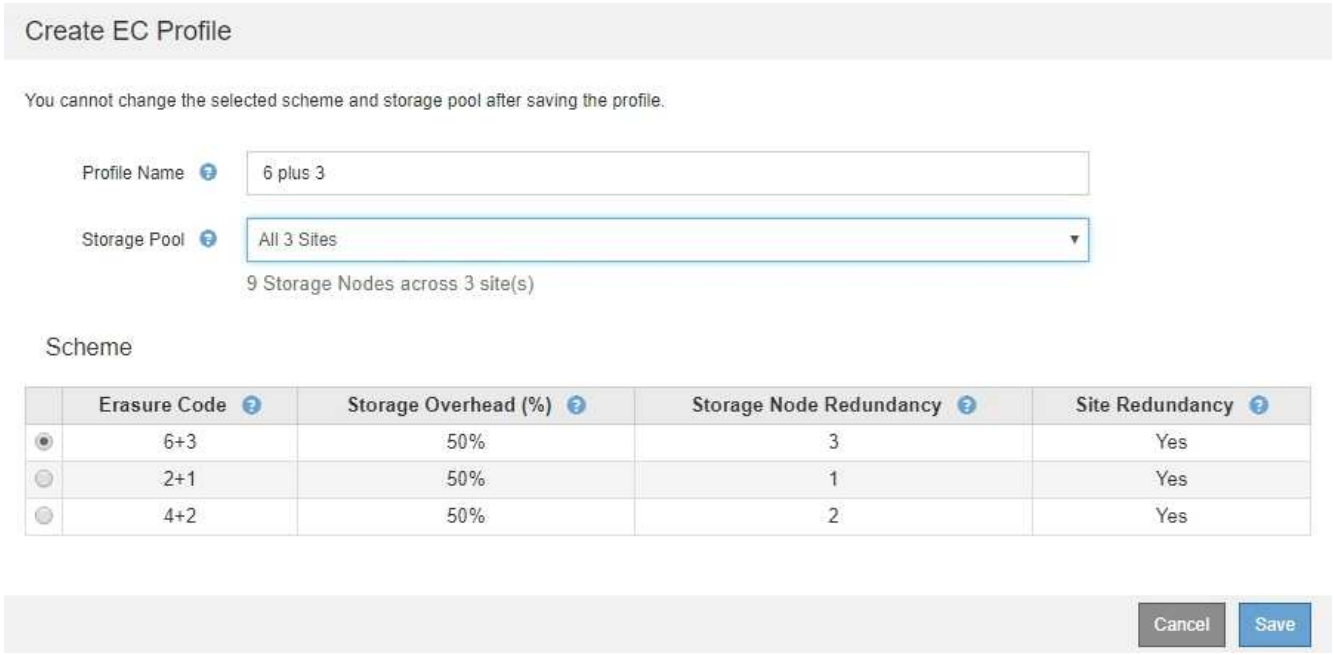
> O nome do perfil de codificação de apagamento é anexado ao nome do pool de armazenamento na instrução de colocação de uma regra ILM.

4. Selecione o pool de armazenamento que você criou para esse perfil de codificação de apagamento.

> Se a grade incluir apenas um local no momento, você será impedido de usar o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o site padrão, todos os sites. Esse comportamento impede que o perfil de codificação de apagamento se torne inválido se um segundo site for adicionado.

Se um pool de armazenamento incluir exatamente dois locais, 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.

Quando você seleciona um pool de storage, a lista de esquemas de codificação de apagamento disponíveis é exibida, com base no número de nós de storage e sites no pool.



As seguintes informações são listadas para cada esquema de codificação de apagamento disponível:

- **Código de apagamento**: O nome do esquema de codificação de apagamento no seguinte formato: Fragmentos de dados e fragmentos de paridade.
- * Sobrecarga de armazenamento (%)*: O armazenamento adicional necessário para fragmentos de paridade em relação ao tamanho de dados do objeto. Sobrecarga de armazenamento: Número total de fragmentos de paridade / número total de fragmentos de dados.
- **Redundância do nó de storage**: O número de nós de storage que podem ser perdidos, mantendo a capacidade de recuperar dados de objeto.
- **Redundância do site**: Se o código de apagamento selecionado permite que os dados do objeto sejam recuperados se um site for perdido.

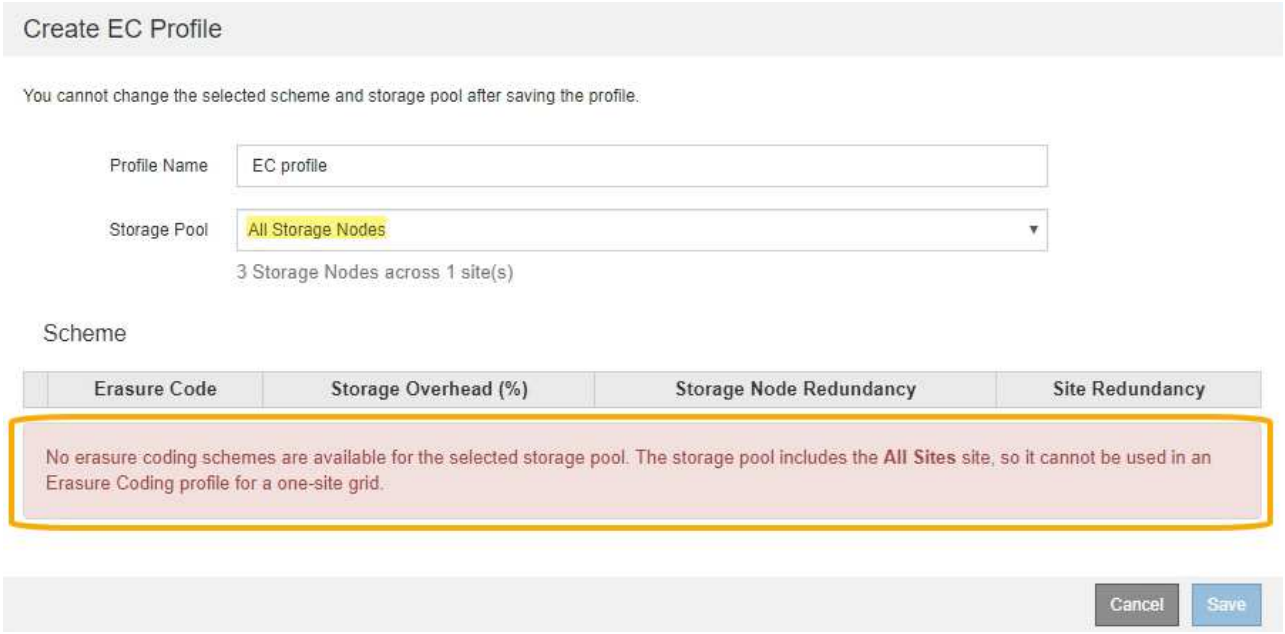
  Para dar suporte à redundância de sites, o pool de storage selecionado deve incluir vários locais, cada um com nós de storage suficientes para permitir que qualquer site seja perdido. Por exemplo, para oferecer suporte à redundância de sites usando um 6 esquema de codificação de apagamento de mais de 3 horas por dia, o pool de storage selecionado deve incluir pelo menos três locais com pelo menos três nós de storage em cada local.

  As mensagens são exibidas nestes casos:

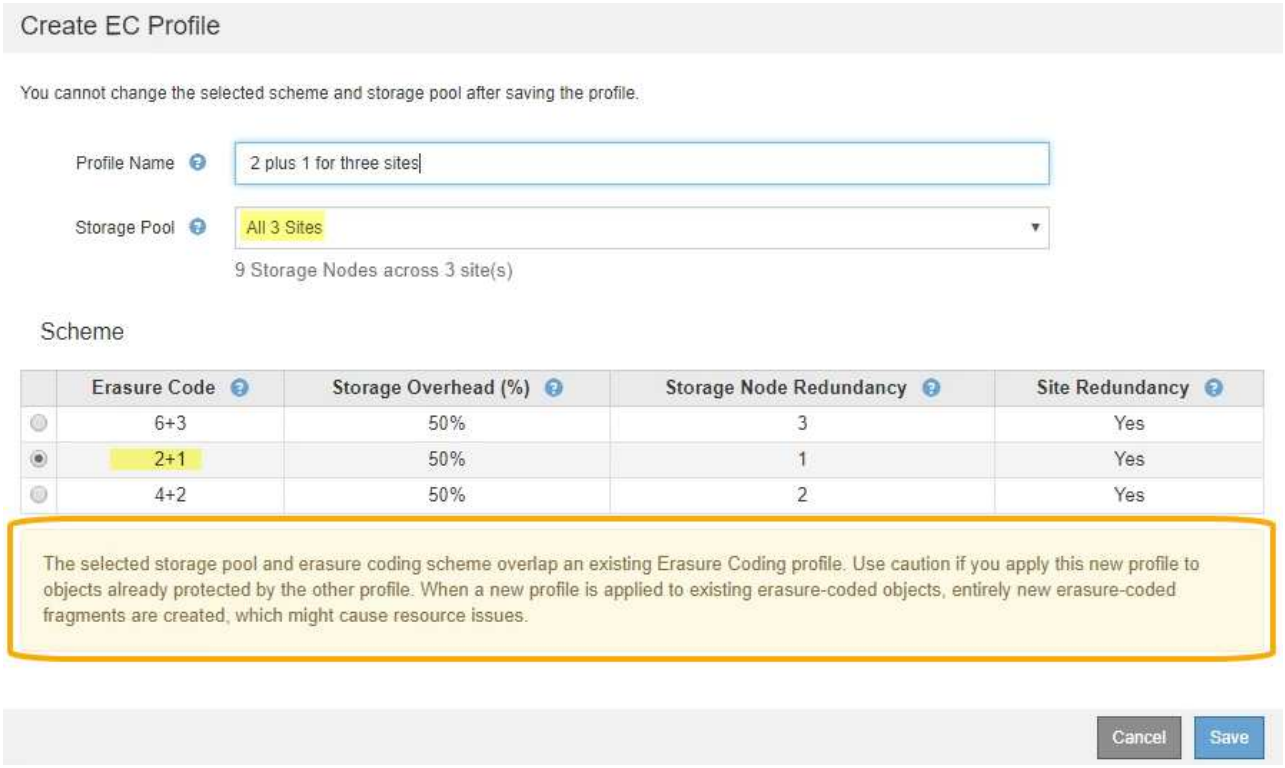
- O pool de armazenamento selecionado não fornece redundância de site. A mensagem a seguir é esperada quando o pool de armazenamento selecionado inclui apenas um local. Você pode usar esse perfil de codificação de apagamento nas regras do ILM para proteger contra falhas de nós.

- O pool de storage selecionado não atende aos requisitos de qualquer esquema de codificação de apagamento. Por exemplo, a seguinte mensagem é esperada quando o pool de armazenamento selecionado inclui exatamente dois locais. Para usar a codificação de apagamento para proteger os dados de objetos, selecione um pool de storage com exatamente um local ou um pool de storage com três ou mais locais.

- Sua grade inclui apenas um local e você selecionou o pool de storage padrão, todos os nós de storage ou qualquer pool de storage que inclua o local padrão, todos os sites.



- O esquema de codificação de apagamento e o pool de storage selecionado se sobrepõem a outro perfil de codificação de apagamento.



Neste exemplo, uma mensagem de aviso aparece porque outro perfil de codificação de apagamento está usando o esquema 2-1 e o conjunto de armazenamento para o outro perfil também usa um dos sites no conjunto de armazenamento de todos os 3 sites.

Embora você não seja impedido de criar este novo perfil, você deve ter muito cuidado ao começar a usá-lo na política ILM. Se esse novo perfil for aplicado a objetos codificados de apagamento já protegidos pelo outro perfil, o StorageGRID criará um conjunto totalmente novo de fragmentos de objeto. Ele não reutilizará os 2 fragmentos existentes. 1. Problemas de recursos podem ocorrer quando você migra de um perfil de codificação de apagamento para o outro, mesmo que os esquemas de codificação de apagamento sejam os mesmos.

5. Se mais de um esquema de codificação de apagamento estiver listado, selecione o que deseja usar.

   Ao decidir qual esquema de codificação de apagamento usar, você deve equilibrar a tolerância a falhas (alcançada por ter mais segmentos de paridade) com os requisitos de tráfego de rede para reparos (mais fragmentos equivale a mais tráfego de rede). Por exemplo, ao decidir entre um esquema 4-2 e um esquema 6-3, selecione o esquema 6-3 se forem necessárias paridade adicional e tolerância a falhas. Selecione o esquema 4 mais 2 se os recursos de rede forem restritos para reduzir o uso da rede durante reparos de nó.

6. Clique em **Salvar**.

Renomeando 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.

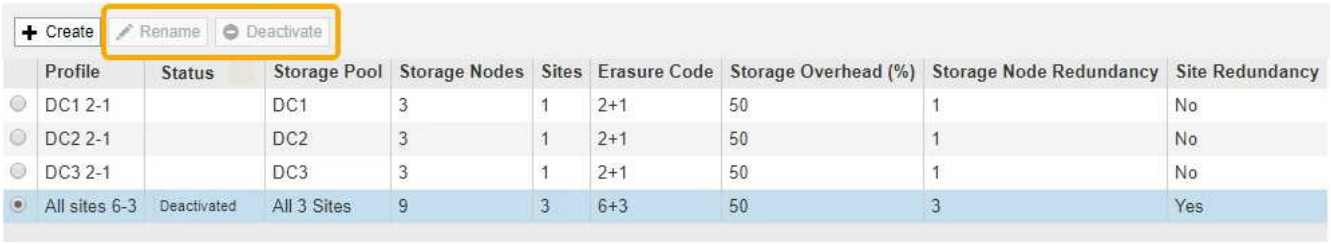
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **ILM** > **Codificação de apagamento**.

   A página Perfis de codificação de apagamento é exibida. Os botões **Renomear** e **Desativar** estão desativados.



	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	DC1 2-1		DC1	3	1	2+1	50	1	No
○	DC2 2-1		DC2	3	1	2+1	50	1	No
○	DC3 2-1		DC3	3	1	2+1	50	1	No
◉	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Selecione o perfil que deseja renomear.

   Os botões **Renomear** e **Desativar** ficam ativados.

3. Clique em **Renomear**.

   A caixa de diálogo Renomear perfil EC é exibida.

4. Introduza 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. Clique em **Salvar**.

Desativar um perfil de codificação de apagamento

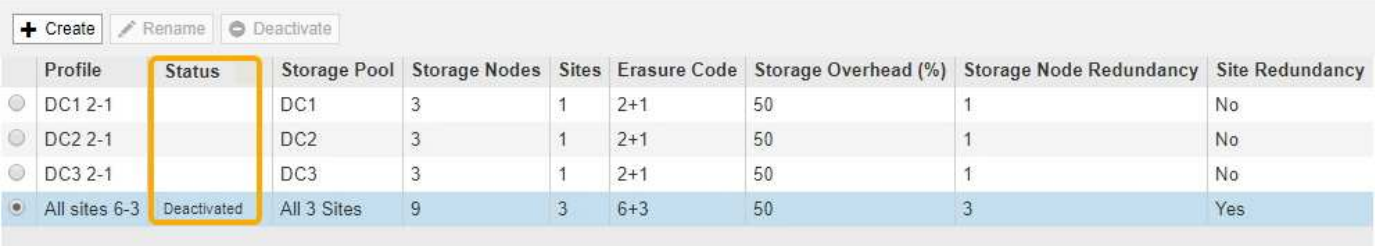
Você pode desativar um perfil de codificação de apagamento se você não planeja mais usá-lo e se o perfil não for usado atualmente em nenhuma regra de ILM.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter confirmado que nenhuma operação de reparo de dados codificados de apagamento ou procedimentos de desativação estão em andamento. Uma mensagem de erro é 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
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Já não pode utilizar 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.

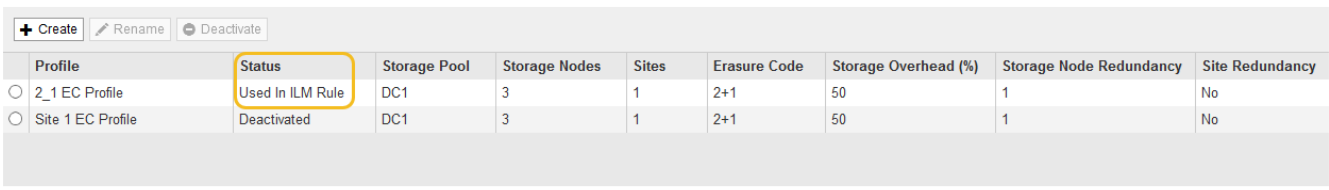
Passos

1. Selecione **ILM** > **Codificação de apagamento**.

   A página Perfis de codificação de apagamento é exibida. Os botões **Renomear** e **Desativar** estão desativados.

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 **2_1 EC Profile** é usado em pelo menos uma regra ILM.



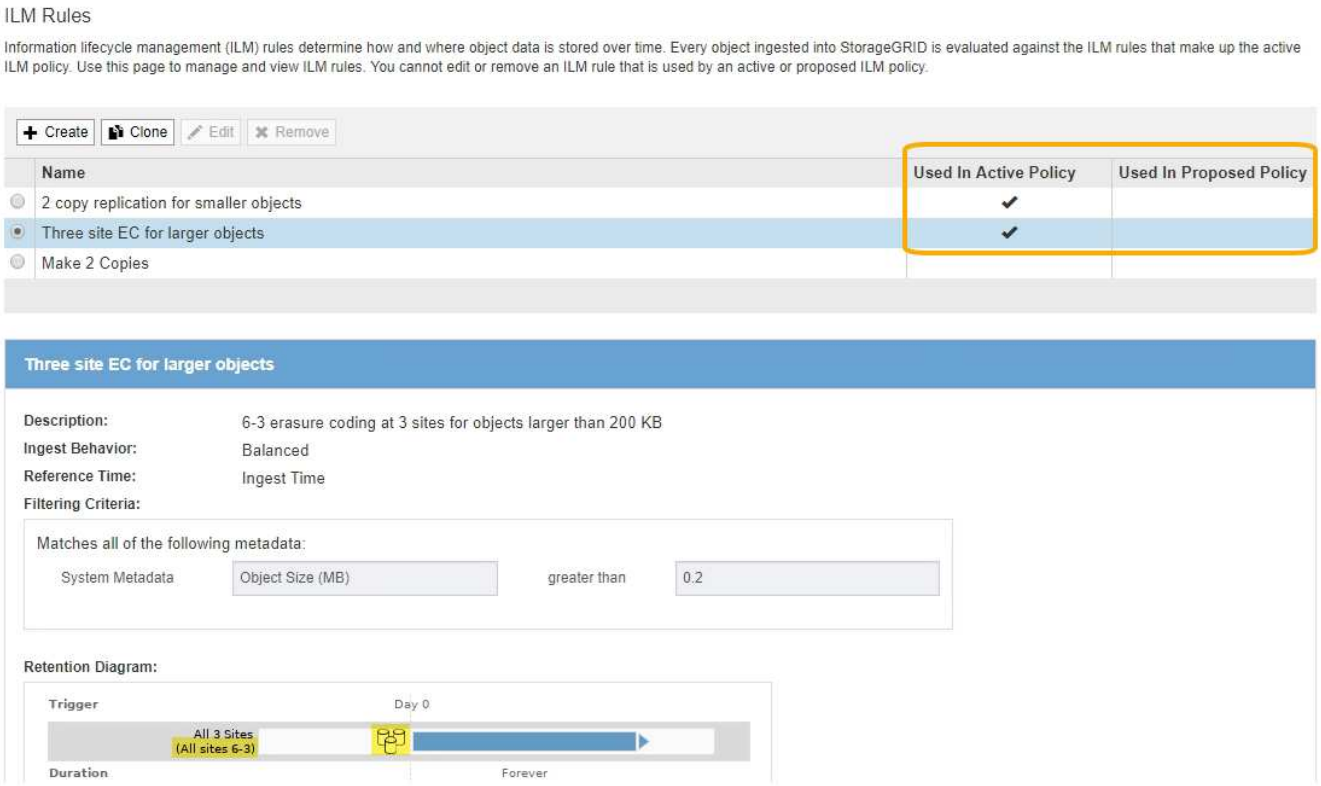
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Se o perfil for usado em uma regra ILM, siga estas etapas:

   a. Selecione **ILM** > **regras**.

b. Para cada regra listada, selecione o botão de opção e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de apagamento que você deseja desativar.

   No exemplo, a regra **Three site EC para objetos maiores** usa um pool de armazenamento chamado **All 3 Sites** e o perfil **All Sites 6-3** Erasure Coding. Os perfis de codificação de apagamento são representados por este ícone:



a. 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.

   No exemplo, a regra **Three site EC para objetos maiores** é usada na política ILM ativa.

b. 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.	*none*
Em uma regra ILM que nunca foi usada em nenhuma política ILM	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.	"Trabalhando com regras de ILM e políticas de 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	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. **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. Embora você possa tentar desativar com segurança um perfil de codificação de apagamento 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. 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.	• "Criando uma política ILM" • "Trabalhando com regras de ILM e políticas de ILM"
Em uma regra ILM que está atualmente em uma política de ILM proposta	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.	• "Criando uma política ILM" • "Trabalhando com regras de ILM e políticas de 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 em uma política ILM histórica	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.	• "Trabalhando com regras de ILM e políticas de ILM"

c. 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter 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 e devem conter pelo menos 2 e não mais de 32 carateres. Os carateres válidos são números, letras e hífens.

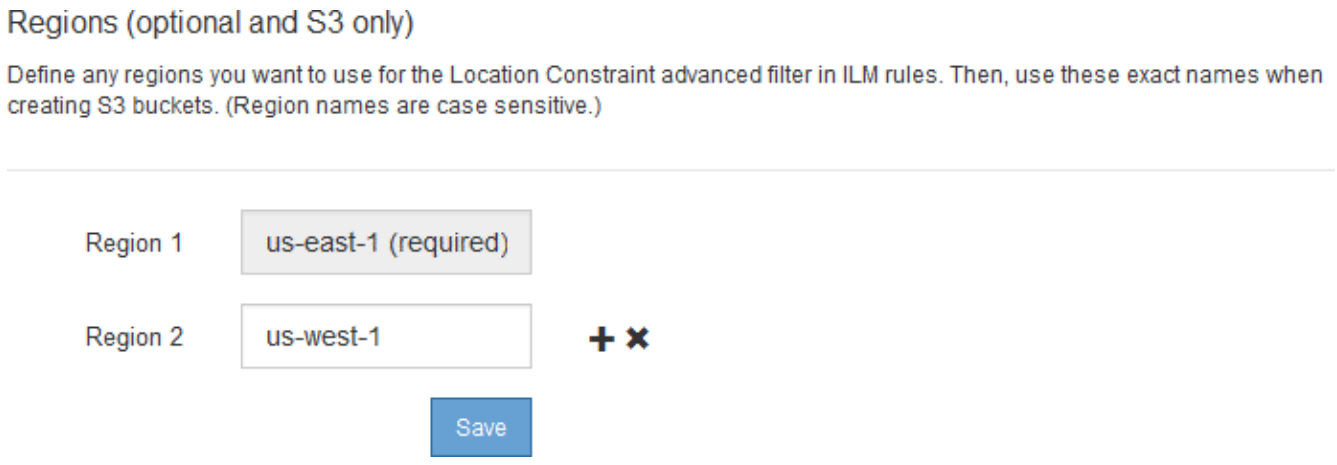
> ⓘ A UE não é considerada um apelido para a ue-oeste-1. Se você quiser usar a região da UE ou da ue-oeste-1, você deve usar o nome exato.

- 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.

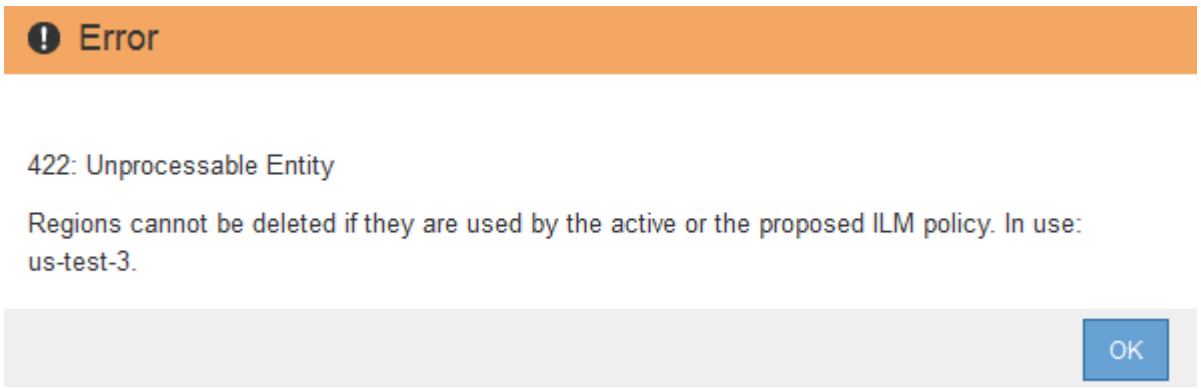


2. Para adicionar uma região:
   a. Clique no ícone de inserção ➕à direita da última entrada.
   b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

      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, clique no ícone de exclusão ✖.

   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, clique em **Salvar**.

   Agora você pode selecionar essas regiões na lista **restrição de localização** na página filtragem avançada do assistente criar regra ILM.

Informações relacionadas

"Usando filtros avançados em regras ILM"

Criando 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 regra ILM.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você quiser especificar a que contas de inquilino esta regra se aplica, você deve ter a permissão Contas de locatário ou você deve saber 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.
- Se você estiver criando cópias replicadas, terá que ter configurado todos os pools de storage ou pools de storage em nuvem que você planeja usar.
- Se estiver criando cópias codificadas para apagamento, você deverá ter configurado um perfil de codificação de apagamento.
- Você deve estar familiarizado com o "opções de proteção de dados para ingestão".

- Se você precisar criar uma regra compatível para usar com o bloqueio de objetos S3, você deve estar familiarizado com o "Requisitos para o bloqueio de objetos S3".

> Para criar a regra ILM padrão para uma política, use este procedimento em vez disso: "Criando uma regra ILM padrão".

Sobre esta tarefa

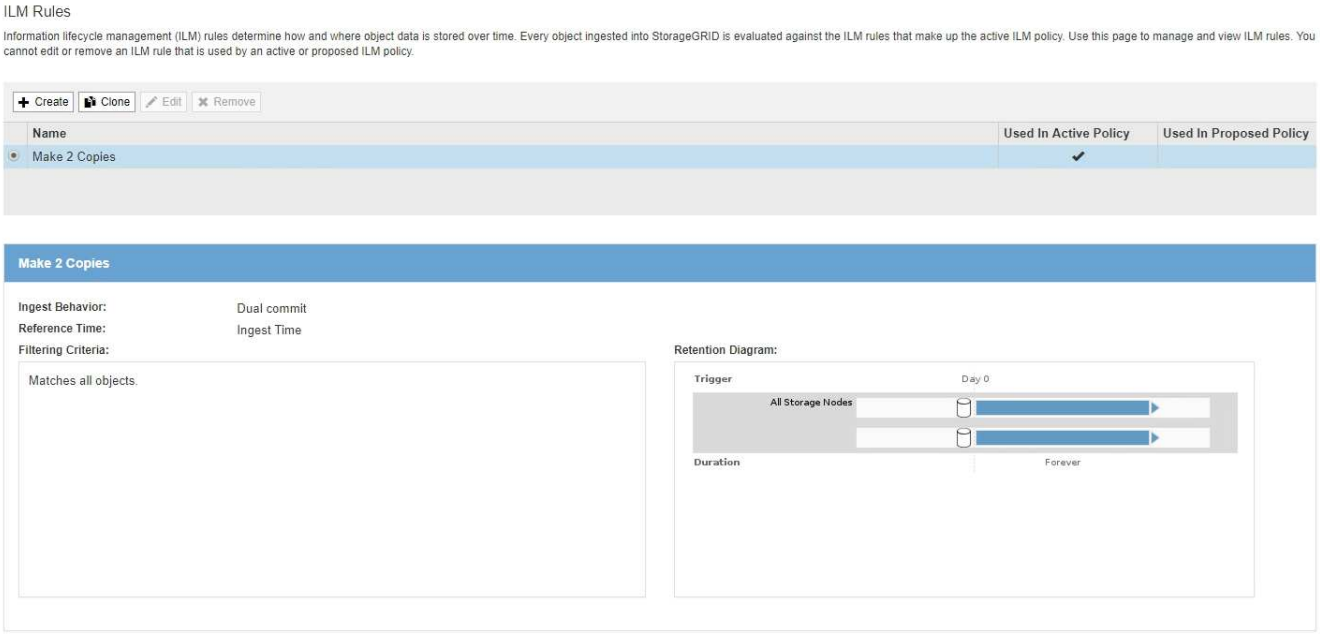
Ao criar regras ILM:

- 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 conetam 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 usar para a opção de proteção de dados na ingestão (Balanced, strict ou Dual Commit)

Passos

1. Selecione **ILM** > **regras**.

   A página ILM Rules (regras do ILM) é exibida, com a regra de estoque, faça 2 cópias, selecionadas.



> A página regras do ILM parece um pouco diferente se a configuração global de bloqueio de objetos do S3 tiver sido ativada para o sistema StorageGRID. A tabela de resumo inclui uma coluna **compliant** e os detalhes da regra selecionada incluem um campo **compliant**.

2. Selecione **criar**.

   A etapa 1 (Definir noções básicas) do assistente criar regra ILM é exibida. Você usa a página Definir noções básicas para definir quais objetos a regra se aplica.

Informações relacionadas

"Use S3"

"Use Swift"

"Configurando perfis de codificação de apagamento"

"Configurando pools de armazenamento"

"Usando Cloud Storage Pools"

"Opções de proteção de dados para ingestão"

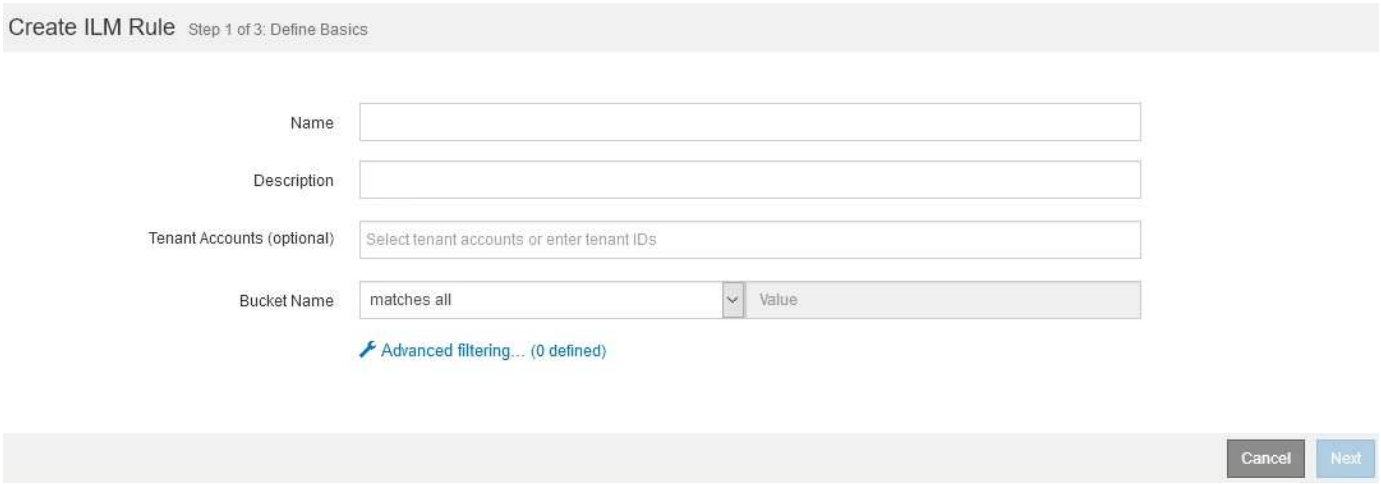
"Gerenciando objetos com o S3 Object Lock"

Passo 1 de 3: Defina o básico

A etapa 1 (Definir noções básicas) do assistente criar regra ILM permite definir os filtros básicos e avançados da regra.

Sobre esta tarefa

Ao avaliar um objeto em relação a uma 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.



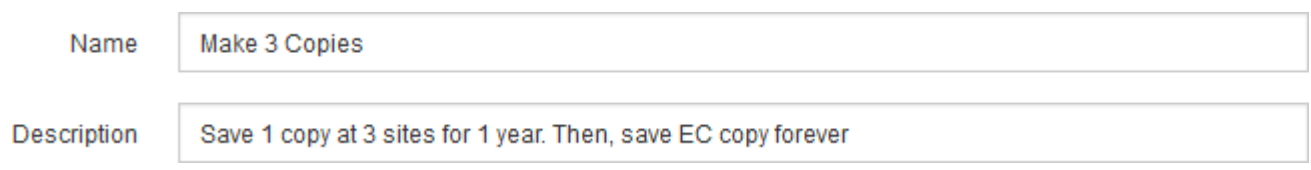
Passos

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

   Tem de introduzir entre 1 e 64 carateres.

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 poderá 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. Opcionalmente, selecione **filtragem avançada** para especificar filtros adicionais.

   Se você não configurar a filtragem avançada, a regra se aplica a todos os objetos que correspondem aos filtros básicos.

   > Se esta regra criar cópias codificadas por apagamento, selecione **filtragem avançada**. Em seguida, adicione o filtro avançado **Object Size (MB)** e defina-o como **maior que 0,2**. O filtro de tamanho garante que os objetos com 2 MB ou menos não serão codificados para apagamento.

6. Selecione **seguinte**.

   É apresentado o passo 2 (Definir posicionamentos).

Informações relacionadas

"O que é a filtragem de regras ILM"

"Usando filtros avançados em regras ILM"

"Passo 2 de 3: Definir posicionamentos"

Usando filtros avançados em regras 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.

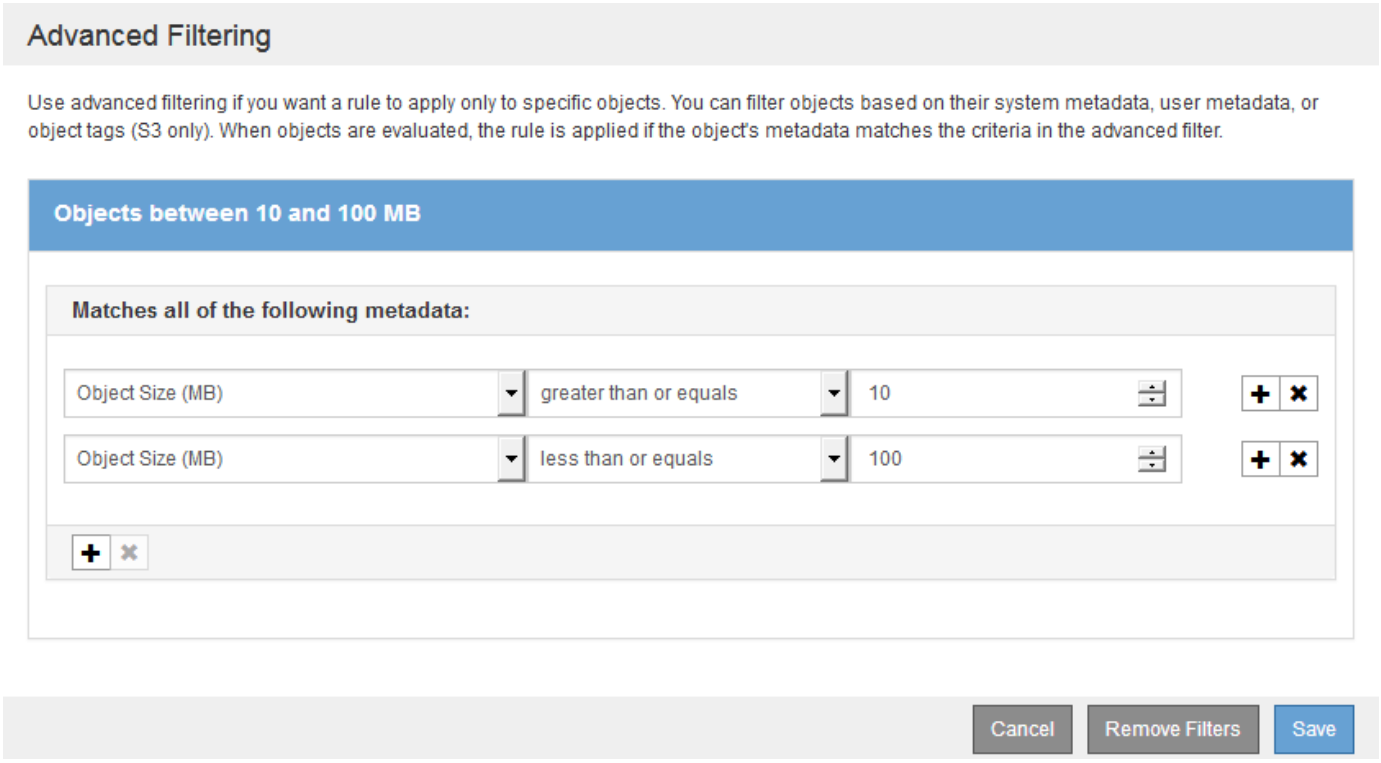
Tipo de metadados	Operadores suportados	Valor dos metadados
Tempo de ingestão (microssegundos)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual	Hora e data em que o objeto foi ingerido. **Observação:** para evitar problemas de recursos ao ativar uma nova política 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.
Chave	• igual a • não é igual • contém • não contém • começa com • não começa com • termina com • não termina com	Toda ou parte de uma chave de objeto S3 ou Swift única. Por exemplo, você pode querer combinar objetos que terminam com `.txt` ou começam `test-object/` com .
Último tempo de acesso (microssegundos)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual • existe • não existe	Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado). **Observação:** se você planeja usar o último tempo de acesso como um filtro avançado, as atualizações do último tempo de acesso devem estar ativadas para o bucket do S3 ou o contentor Swift. "Usando o último tempo de acesso nas regras do ILM"
Restrição de localização (apenas S3)	• igual a • não é igual	A região onde foi criado um bucket S3. Utilize **ILM** > **Regiões** para definir as regiões que são apresentadas. **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)"

Tipo de metadados	Operadores suportados	Valor dos metadados
Tamanho do objeto (MB)	• igual a • não é igual • menos de • menor que ou igual • superior a. • maior que ou igual	O tamanho do objeto em MB. Para filtrar em tamanhos de objetos menores que 1 MB, digite um valor decimal. Por exemplo, defina o filtro avançado **Object Size (MB)** para **maior que 0,2** para qualquer regra que faça cópias codificadas por apagamento. Essa configuração garante que a codificação de apagamento não seja usada para objetos 200 KB ou menores. **Observação:** o tipo de navegador e as configurações de localidade controlam se você precisa usar um ponto ou uma vírgula como separador decimal.
Metadados do utilizador	• contém • termina com • igual a • existe • não contém • não termina com • não é igual • não existe • não começa com • começa com	Par chave-valor, onde **Nome de metadados do usuário** é a chave e **valor de metadados do usuário** é o valor. Por exemplo, para filtrar objetos que têm metadados de usuário do `color=blue`, especifique `color` para **Nome de metadados do usuário**, `equals` para o operador e `blue` para **valor de metadados do usuário**. **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.
Etiqueta de objeto (apenas S3)	• contém • termina com • igual a • existe • não contém • não termina com • não é igual • não existe • não começa com • começa com	Par chave-valor, onde **Nome da etiqueta do objeto** é a chave e **valor da etiqueta do objeto** é o valor. Por exemplo, para filtrar objetos que têm uma tag de objeto de `Image=True`, especifique `Image` para **Nome da Etiqueta de objeto**, `equals` para o operador e `True` para **valor da Etiqueta de objeto**. **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.

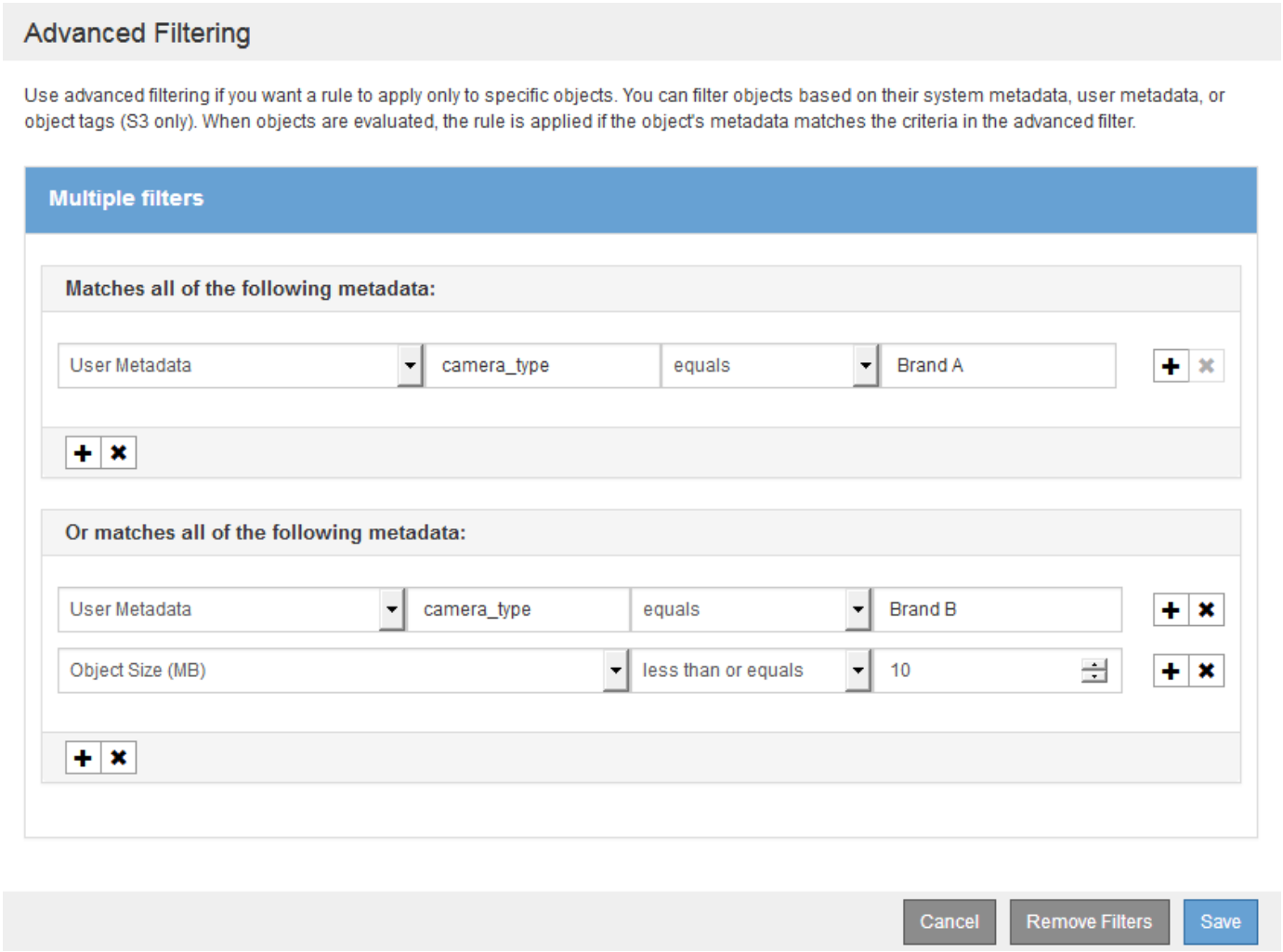
Especificando vários tipos e valores de metadados

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.



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.



Informações relacionadas

"Usando o último tempo de acesso nas regras do ILM"

"Configurar regiões (opcional e apenas S3)"

Passo 2 de 3: Definir posicionamentos

A etapa 2 (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.

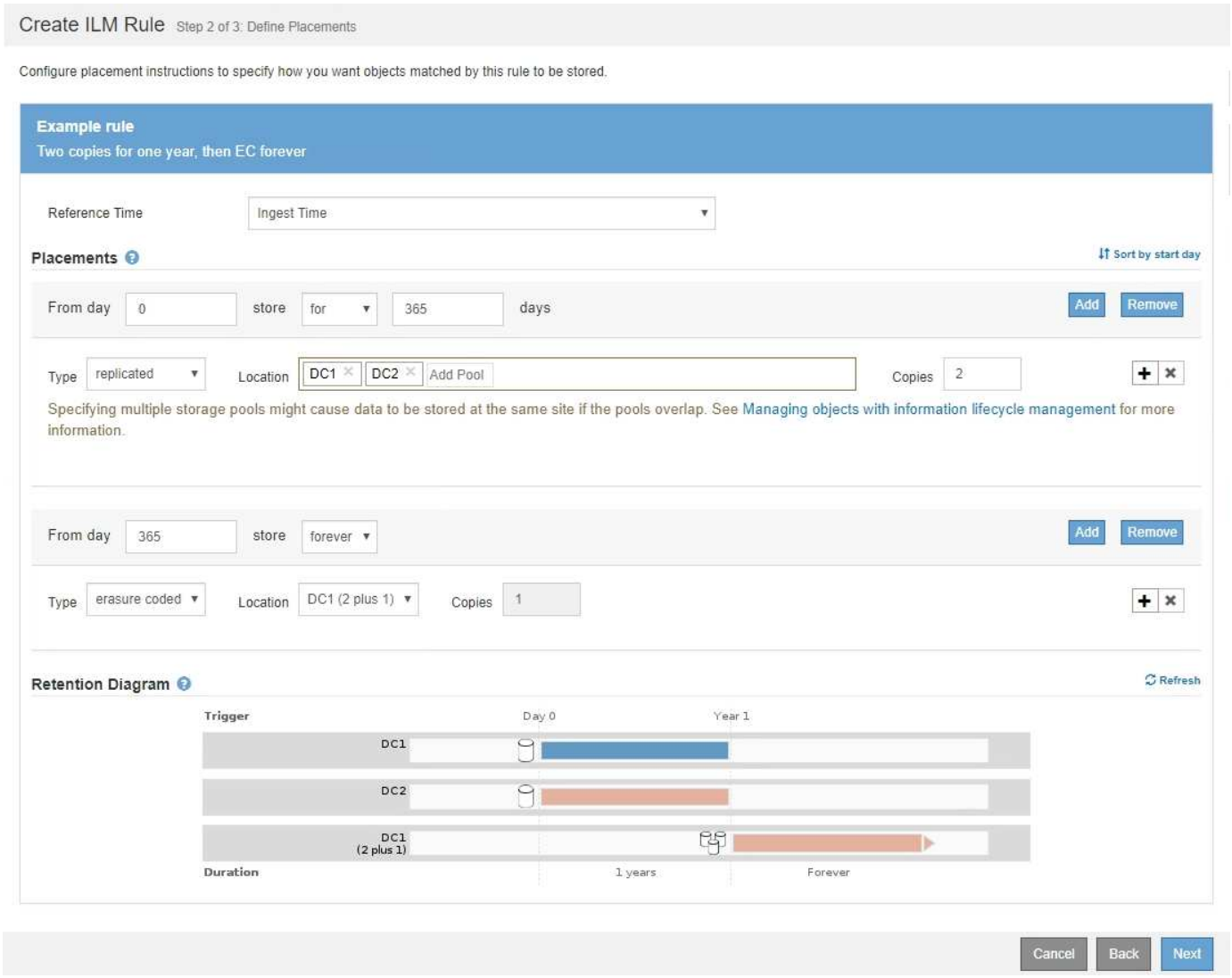
Sobre esta tarefa

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.

Este exemplo de regra ILM cria duas cópias replicadas para o primeiro ano. Cada cópia é salva em um pool de armazenamento em um local diferente. Após um ano, uma cópia codificada por apagamento de 2 mais de

1 é feita e salva em apenas um local.



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 contentor Swift. "Usando o último tempo de acesso nas regras do ILM"

Opção	Descrição
Hora não atual	O tempo em que uma versão de objeto se tornou não atual porque uma nova versão foi ingerida e substituída como a versão atual. **Nota:** o tempo não atual aplica-se apenas a objetos S3D em buckets habilitados para versionamento. Você pode usar essa opção para reduzir o impactos de armazenamento de objetos com controle de versão filtrando versões de objetos não atuais. Veja "'exemplo 4: Regras e política do ILM para objetos com versão S3.'"
Tempo de criação definido pelo utilizador	Um tempo especificado nos metadados definidos pelo usuário.

Se você quiser criar uma regra compatível, selecione **tempo de ingestão**.

2. Na seção **colocações**, selecione 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 ("dia 0 para 365 dias"). Pelo menos uma instrução deve começar no dia 0.

3. Se você quiser criar cópias replicadas:
   a. Na lista suspensa **tipo**, selecione **replicado**.
   b. No campo **localização**, selecione **Adicionar pool** para cada pool de armazenamento que você 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 sua grade incluir três nós de storage e você selecionar 4 como o número de cópias, apenas três cópias serão feitas - uma cópia para cada nó de storage.

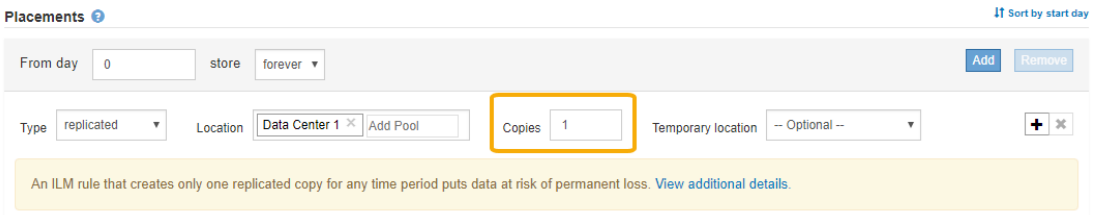
      O alerta **ILM Placement Unachievable** é acionado para indicar que a regra ILM não pôde ser completamente aplicada.

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

      - O número de cópias não pode ser maior 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 do que o número de pools de storage, o sistema distribui as cópias para manter o uso do disco entre os pools balanceado e garantir 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 padrão de todos os nós de storage e outro pool de storage.

c. 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. Se existir apenas uma cópia replicada de um objeto durante um período de tempo, 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.



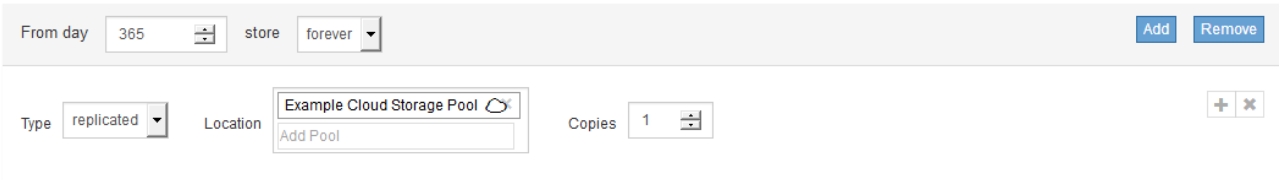
Para evitar esses riscos, faça um ou mais dos seguintes procedimentos:

- Aumente o número de cópias para o período de tempo.
- Clique no ícone de sinal de adição + para criar cópias adicionais durante o período de tempo. Em seguida, selecione um pool de armazenamento diferente ou um pool de armazenamento em nuvem.
- Selecione **codificar para apagamento** para tipo, em vez de **replicado**. Você pode ignorar esse aviso com segurança se essa regra já criar várias cópias para todos os períodos de tempo.

d. Se você especificou apenas um pool de armazenamento, ignore o campo **local temporário**.

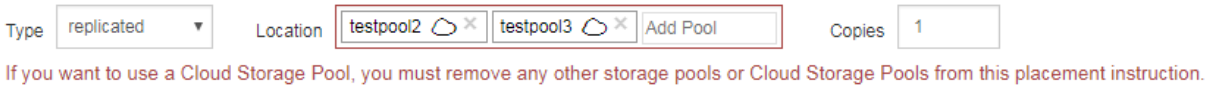
Os locais temporários são obsoletos e serão removidos em uma versão futura.

4. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:
   a. Na lista suspensa **tipo**, selecione **replicado**.
   b. No campo **localização**, selecione **Adicionar Piscina**. Em seguida, selecione um pool de armazenamento em nuvem.

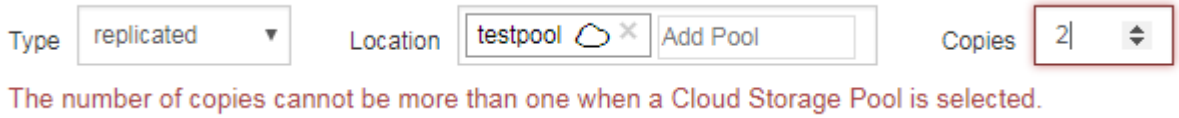


Ao usar Cloud Storage Pools, tenha em mente estas regras:

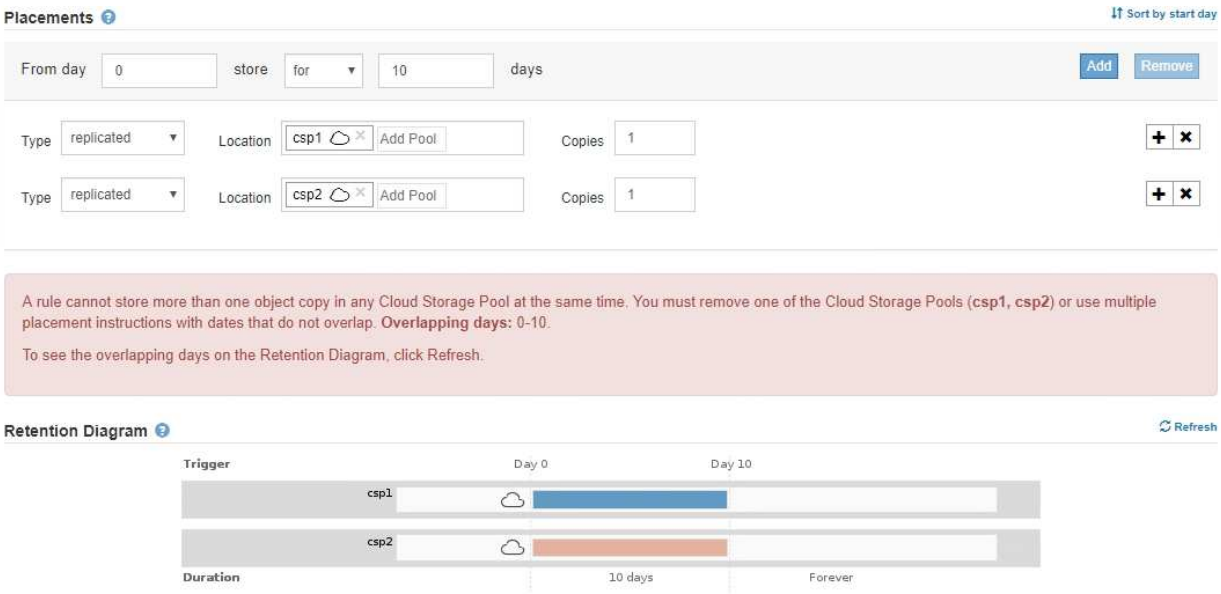
- Você não pode selecionar mais de um pool de armazenamento em nuvem em uma única instrução de colocação. Da mesma forma, você não pode selecionar um pool de armazenamento em nuvem e um pool de armazenamento na mesma instrução de colocação.



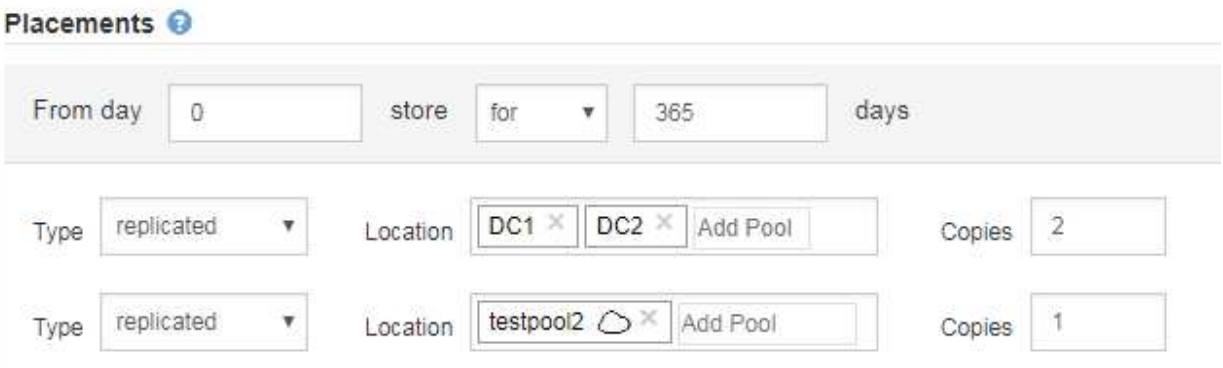
- Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro será exibida se você definir **Copies** como 2 ou mais.



- 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, como este exemplo mostra, 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.



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

   a. Na lista suspensa **Type**, selecione **Erasure Coded**.

      O número de cópias muda para 1. Um aviso será exibido se a regra não tiver um filtro avançado para ignorar objetos com 200 KB ou menos.

      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 o aviso de tamanho do objeto aparecer, siga estas etapas para limpá-lo:

      i. Selecione **voltar** para voltar ao passo 1.

      ii. Selecione **filtragem avançada**.

      iii. Defina o filtro tamanho do objeto (MB) como "'maior que 0,2"".

   c. Selecione o local de armazenamento.

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

6. Opcionalmente, adicione períodos de tempo diferentes ou crie cópias adicionais em locais diferentes:
   - Clique no ícone de mais para criar cópias adicionais em um local diferente durante o mesmo período de tempo.
   - Clique em **Add** para adicionar um período de tempo diferente às instruções de colocação.

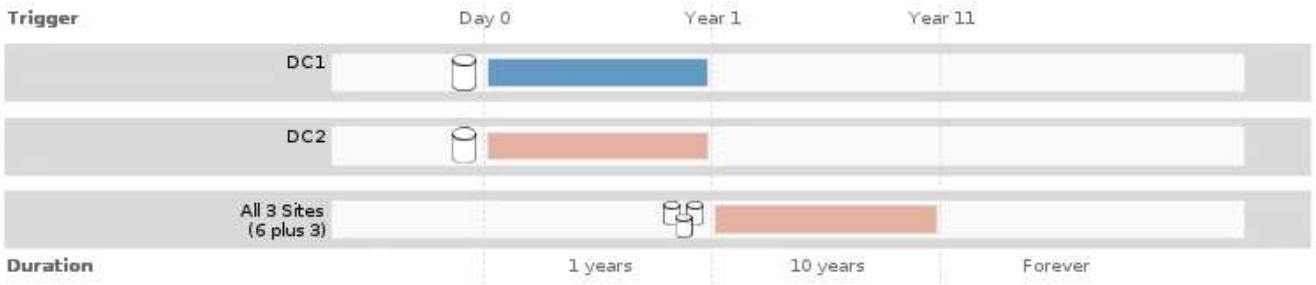
   Os objetos são automaticamente excluídos no final do período de tempo final, a menos que o período de tempo final termine com **Forever**.

7. Clique em **Refresh** para atualizar o Diagrama de retenção e confirmar as instruções de colocação.

Cada linha no diagrama mostra onde e quando cópias de objetos serão colocadas. O tipo de cópia é representado por um dos seguintes ícones:

	Cópia replicada
	Com codificação de apagamento
	Cópia do Cloud Storage Pool

Neste exemplo, duas cópias replicadas serão salvas em dois pools de armazenamento (DC1 e DC2) por um ano. Em seguida, uma cópia codificada por apagamento será salva por mais 10 anos, usando um esquema de codificação de apagamento de mais de 6 3 em três locais. Após 11 anos, os objetos serão excluídos do StorageGRID.



8. Clique em **seguinte**.

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

Informações relacionadas

"Quais são as instruções de colocação de regras do ILM"

"Exemplo 4: Regras ILM e política para objetos com versão S3"

"Por que você não deve usar replicação de cópia única"

"Gerenciando objetos com o S3 Object Lock"

"Usando um pool de armazenamento como um local temporário (obsoleto)"

"Etapa 3 de 3: Definir o comportamento de ingestão"

Usando 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. Você pode usar o Gerenciador do Locatário ou a API de Gerenciamento do Locatário.

> 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 impactos 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	• Não, para a cópia de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Pedido para concluir um carregamento multipart	Sim, para o objeto montado	Sim, para o objeto montado

Informações relacionadas

"Use S3"

"Use uma conta de locatário"

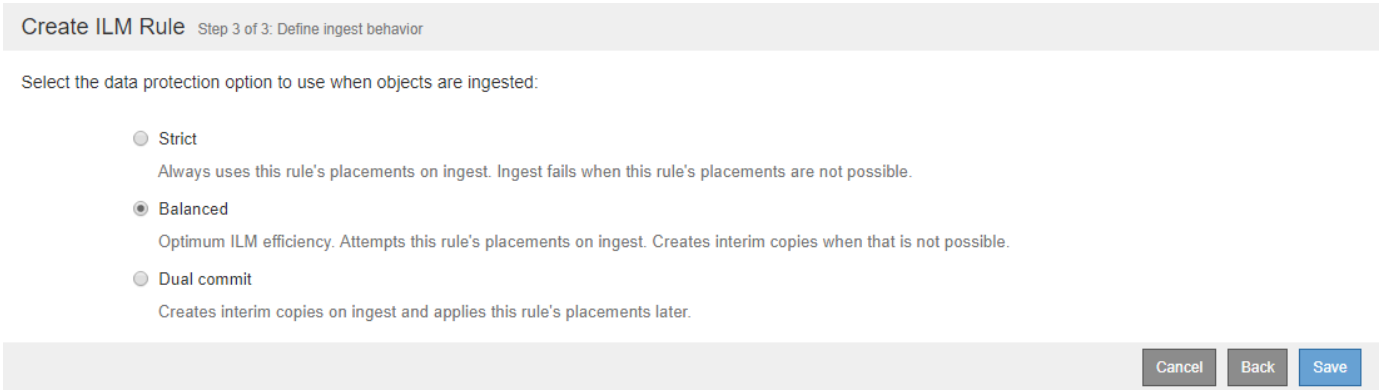
Etapa 3 de 3: Definir o comportamento de ingestão

A etapa 3 (Definir comportamento de ingestão) do assistente criar regra ILM permite que você escolha 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 opção de proteção de dados a ser usada quando os objetos são ingeridos:

Opção	Descrição
Rigoroso	Sempre usa os posicionamentos desta regra na ingestão. A ingestão falha quando os posicionamentos desta regra não são possíveis.
Equilibrado	Eficiência ideal de ILM. Tenta os posicionamentos desta regra na ingestão. Cria cópias provisórias quando isso não é possível.
Commit duplo	Cria cópias provisórias na ingestão e aplica os posicionamentos desta regra mais tarde.

   O Balanced oferece uma combinação adequada de segurança e eficiência dos dados na maioria dos casos. Strict ou Dual Commit são geralmente usados para atender a requisitos específicos.

   Consulte "quais são as opções de proteção de dados para ingestão" e "vantagens e desvantagens de cada opção de proteção de dados" para obter mais informações.

   > Uma mensagem de erro será exibida se você selecionar a opção estrita ou equilibrada e 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

2. Clique em **Salvar**.

   A regra ILM é salva. A regra não se torna ativa até que seja adicionada a uma política ILM e essa política seja ativada.

Informações relacionadas

"Opções de proteção de dados para ingestão"

"Vantagens, desvantagens e limitações das opções de proteção de dados"

"Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"

"Criando uma política ILM"

Criando uma regra ILM padrão

Cada política de ILM deve ter uma regra padrão que não filtra objetos. Antes de criar uma política ILM, você deve criar pelo menos uma regra ILM que possa ser usada como regra padrão para a política.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter 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.

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

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 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**.

   A página regras do ILM é exibida.

2. Selecione **criar**.

   A etapa 1 (Definir noções básicas) do assistente criar regra ILM é exibida.

3. Digite um nome exclusivo para a regra no campo **Nome**.
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 o campo **Bucket Name** em branco.

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

7. Não selecione **filtragem avançada**

   A regra padrão não pode especificar nenhum filtro.

8. Selecione **seguinte**.

   É apresentado o passo 2 (Definir posicionamentos).

9. 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 retiver 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 objeto não podem ser salvas em um pool de storage de nuvem.
     - As cópias de objeto não podem ser guardadas nos nós de arquivo.
     - Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando o tempo de ingestão como o tempo de referência.
     - Pelo menos uma linha das instruções de colocação deve ser "para sempre".
10. Clique em **Refresh** para atualizar o Diagrama de retenção e confirmar as instruções de colocação.
11. Clique em **seguinte**.

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

12. Selecione a opção de proteção de dados a ser usada quando os objetos são ingeridos e selecione **Salvar**.

Criando uma política ILM

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 irrecuperável. 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.

Considerações para criar uma política ILM

- Utilize a política incorporada do sistema, a Política de cópias da linha de base 2, apenas em sistemas de teste. A regra fazer cópias 2 nesta política usa o pool de storage 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.
- 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, essa regra não será avaliada 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.

Informações relacionadas

"O que é uma política ILM"

"Exemplo 6: Alterando uma política ILM"

Criando uma política proposta de ILM

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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter permissões de acesso específicas.
- Você deve ter criado as regras ILM que 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 deve ter criado uma regra ILM padrão para a política que não contém nenhum filtro.

  "Criando uma regra ILM padrão"

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 que se referem ao site.
- Você adicionou um novo locatário com requisitos especiais de proteção de dados.
- Você começou a usar um Cloud Storage Pool.

Utilize a política incorporada do sistema, a Política de cópias da linha de base 2, apenas em sistemas de teste. A regra fazer cópias 2 nesta política usa o pool de storage 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.

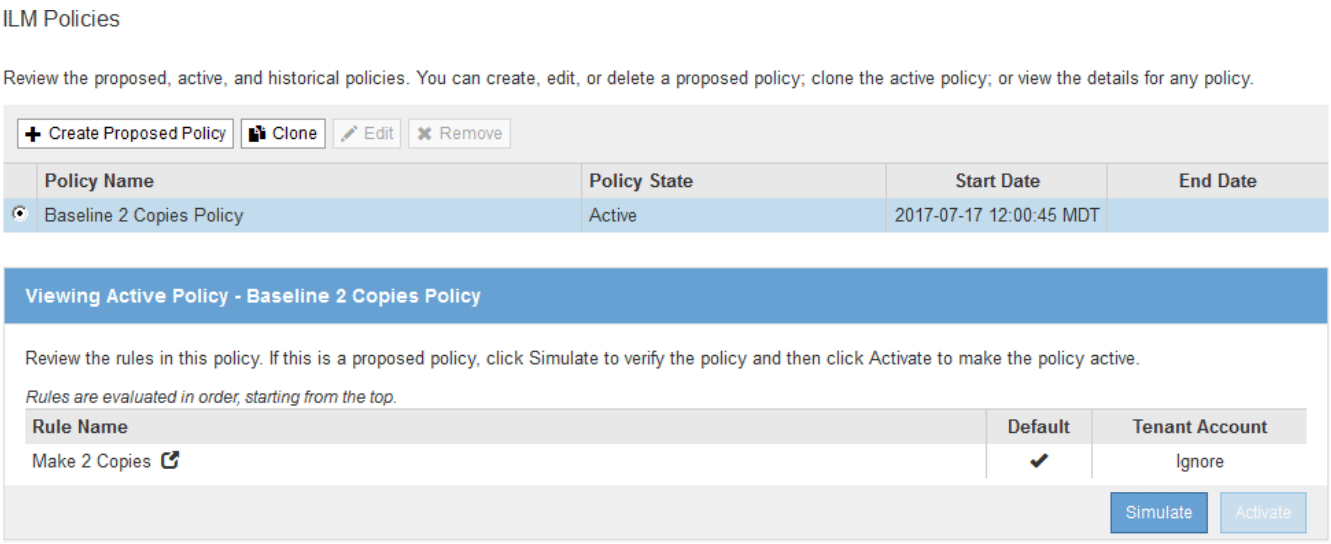
Se a configuração global S3 Object Lock tiver sido ativada, as etapas para criar uma política serão ligeiramente diferentes. Você deve garantir que a política ILM esteja em conformidade com os requisitos de buckets que têm o bloqueio de objeto S3 ativado.

"Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado"

Passos

1. Selecione **ILM** > **políticas**.

   É apresentada a página ILM Policies (políticas ILM). Nesta página, você pode revisar a lista de políticas propostas, ativas e históricas; criar, editar ou remover uma política proposta; clonar a política ativa; ou exibir os detalhes de qualquer política.

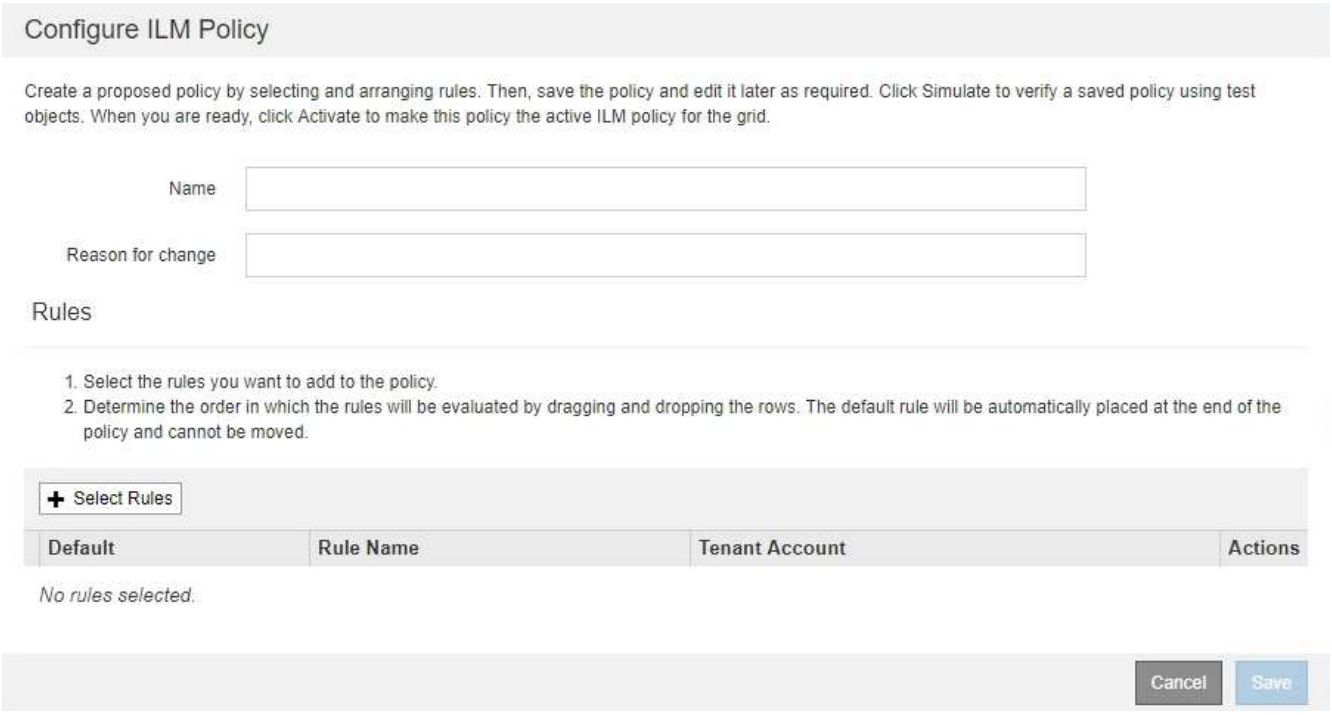


2. Determine como você deseja criar a política de ILM proposta.

Opção	Passos
Crie uma nova política proposta que não tenha regras já selecionadas	a. Se uma política de ILM proposta existir atualmente, selecione essa política e clique em **Remover**. Não é possível criar uma nova política proposta se uma política proposta já existir. b. Clique em **criar política proposta**.
Criar uma política proposta com base na política ativa	a. Se uma política de ILM proposta existir atualmente, selecione essa política e clique em **Remover**. Você não pode clonar a política ativa se uma política proposta já existir. b. Selecione a política ativa na tabela. c. Clique em **Clone**.
Edite a política proposta existente	a. Selecione a política proposta na tabela. b. Clique em **Editar**.

A caixa de diálogo Configurar política ILM é exibida.

Se você estiver criando uma nova política proposta, todos os campos estarão em branco e nenhuma regra será selecionada.



Se você estiver clonando a política ativa, o campo **Name** mostra o nome da política ativa, anexado por um número de versão ("'v2'" no exemplo). As regras usadas na política ativa são selecionadas e mostradas

em sua ordem atual.

3. Digite um nome exclusivo para a política proposta no campo **Nome**.

   Você deve inserir pelo menos 1 e não mais de 64 carateres. Se você estiver clonando a política ativa, poderá usar o nome atual com o número de versão anexado ou inserir um novo nome.

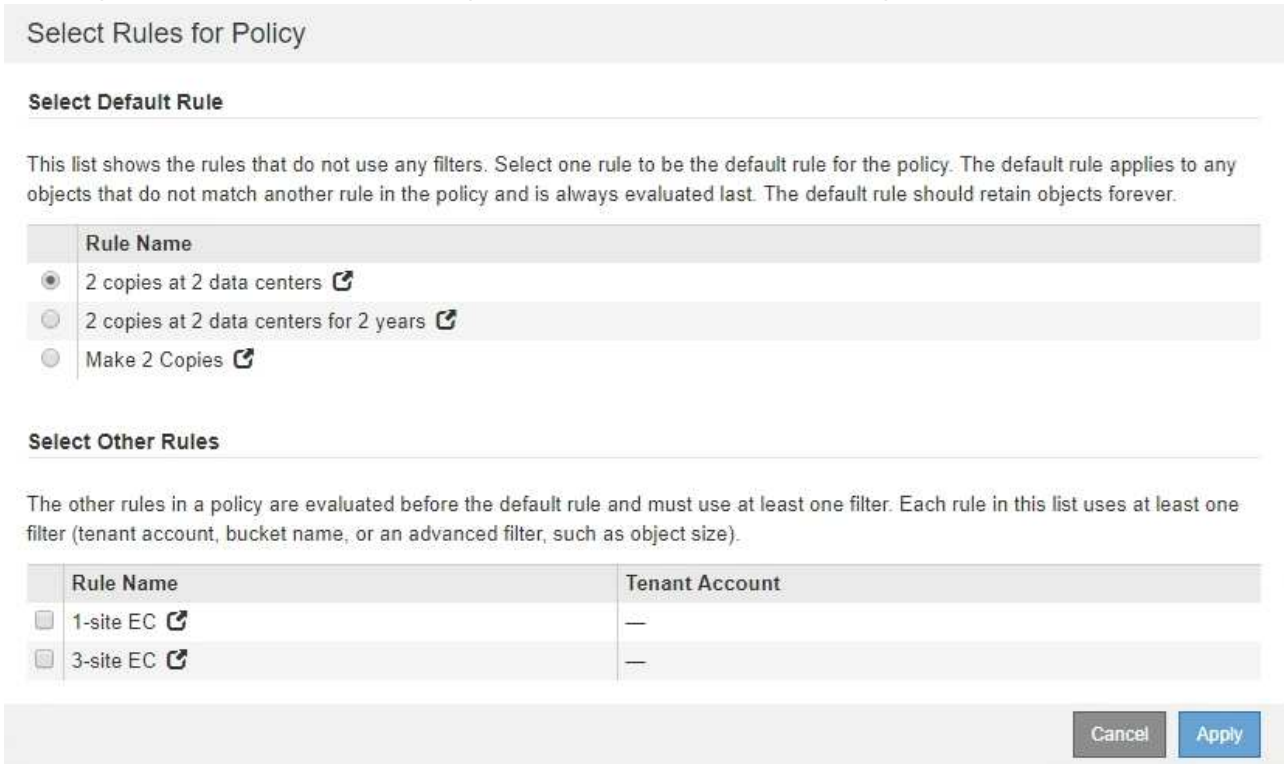
4. Insira o motivo pelo qual você está criando uma nova política proposta no campo **motivo da mudança**.

   Você deve inserir pelo menos 1 e não mais de 128 carateres.

5. Para adicionar regras à política, selecione **Selecionar regras**.

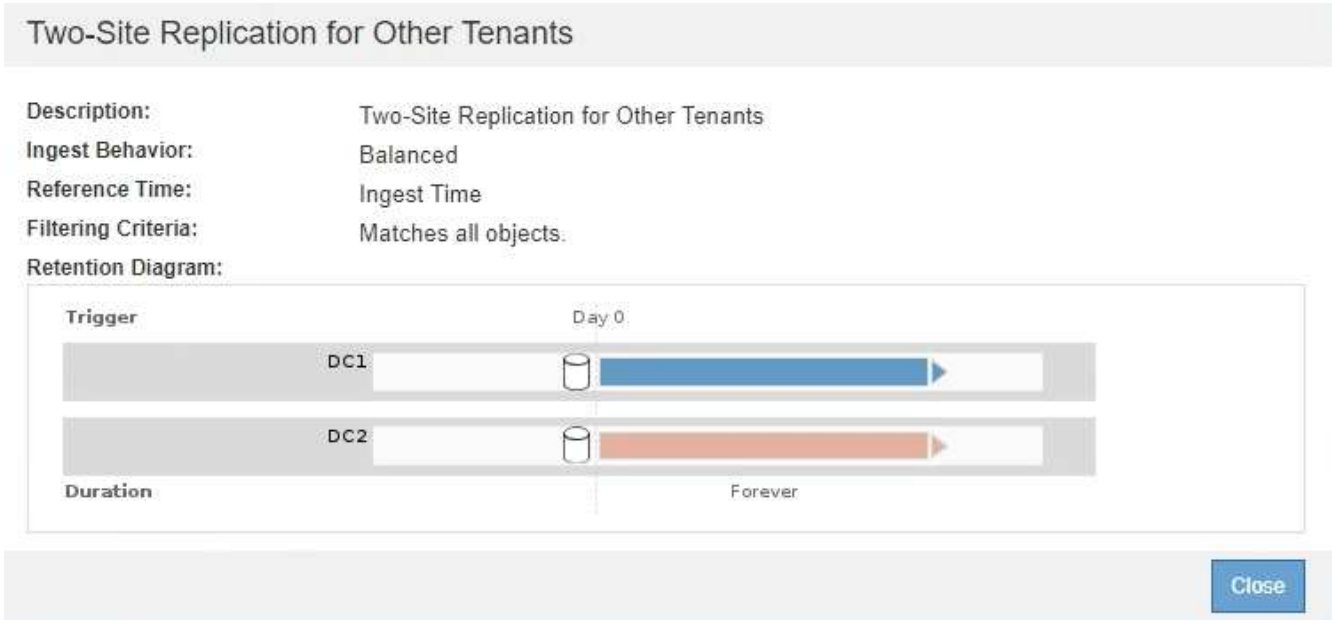
   A caixa de diálogo Selecionar regras para política é exibida, com todas as regras definidas listadas. Se você estiver clonando uma política:

   - 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, um botão permite mover a regra para o final da nova política.



6. Selecione um nome de regra ou o ícone mais detalhes para exibir as configurações dessa regra.

   Este exemplo mostra os detalhes de uma regra ILM que faz duas cópias replicadas em dois sites.



7. Na seção **Selecionar regra padrão**, selecione uma regra padrão para a política proposta.

   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.

   Se nenhuma regra estiver listada na seção Selecionar regra padrão, você deverá sair da página de política ILM e criar uma regra padrão.

   "Criando uma regra ILM padrão"

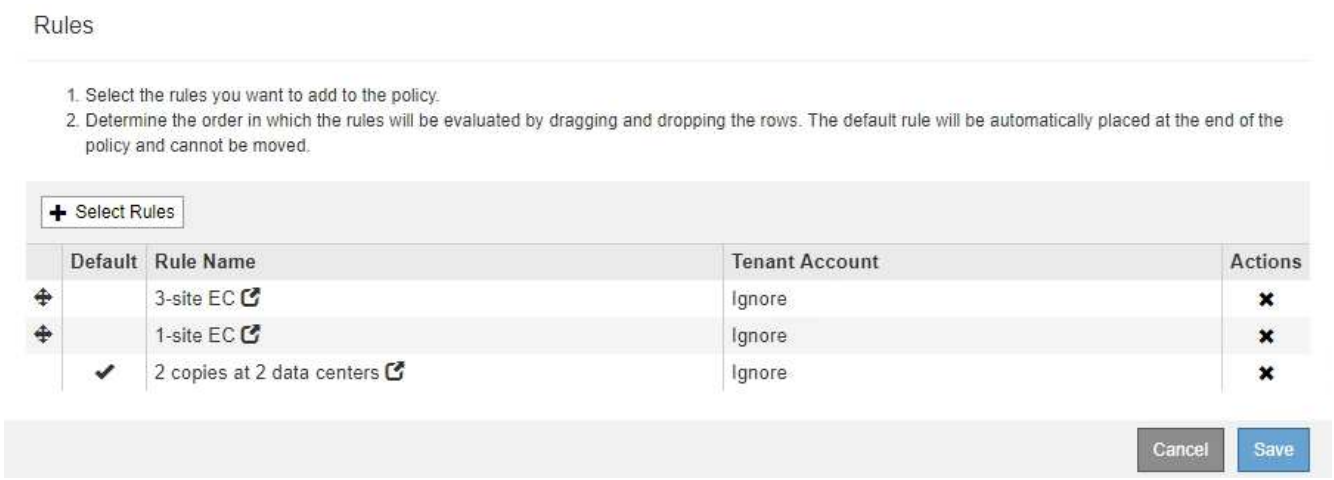
   Não use a regra fazer 2 cópias de estoque como a regra padrão para uma política. A regra fazer 2 cópias usa um único pool de storage, todos os nós de storage, que contém todos os locais. Se o seu sistema StorageGRID tiver mais de um local, duas cópias de um objeto poderão ser colocadas no mesmo local.

8. Na seção **Selecionar outras regras**, selecione quaisquer outras regras que você deseja incluir na política.

   As outras regras são avaliadas antes da regra padrão e devem usar pelo menos um filtro (conta de locatário, nome do intervalo ou um filtro avançado, como tamanho do objeto).

9. Quando terminar de selecionar regras, selecione **aplicar**.

   As regras selecionadas são listadas. A regra padrão está no final, com as outras regras acima dela.



Um aviso aparece se a regra padrão não retiver 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 mais tempo).

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

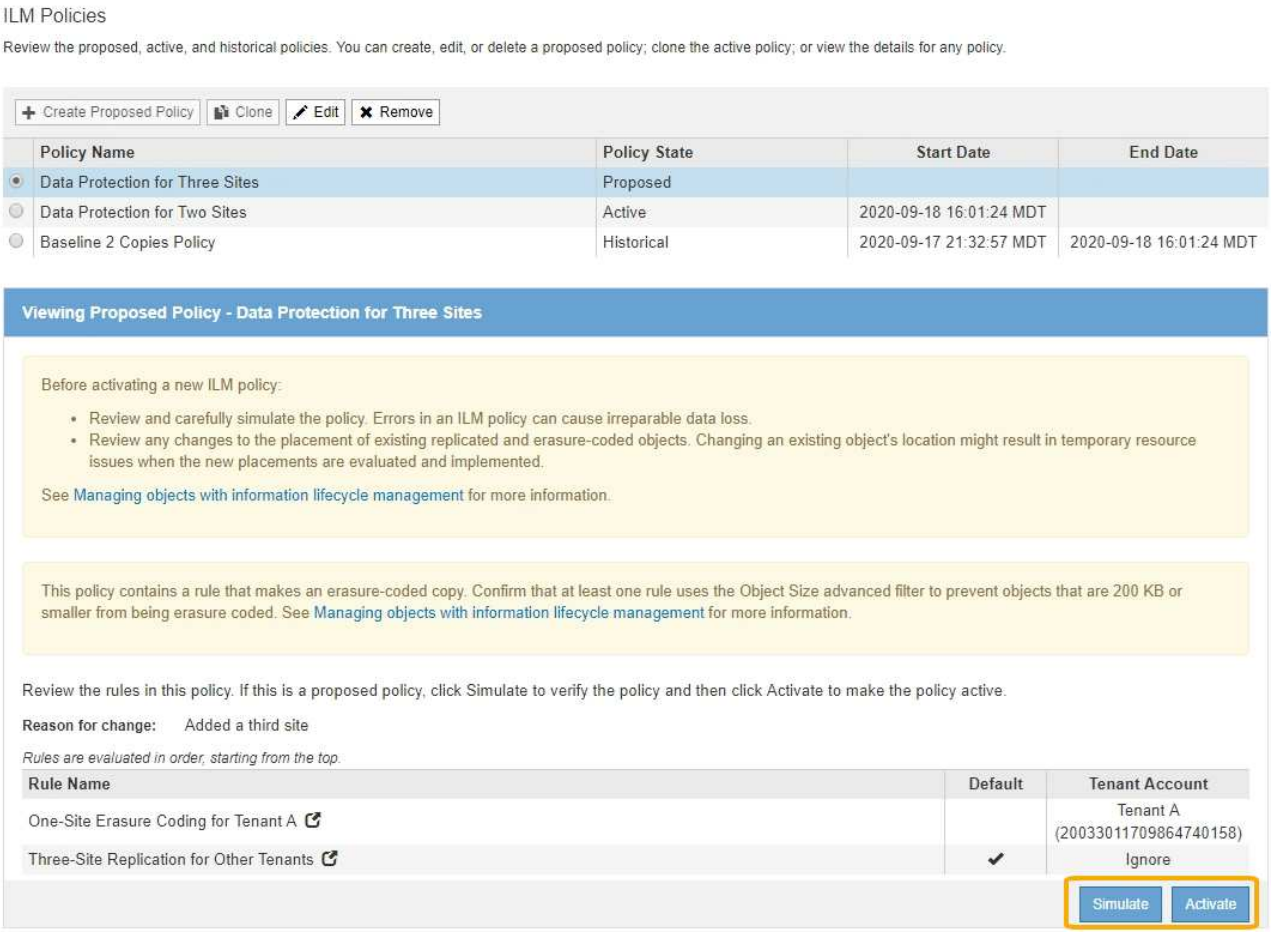
    Não é possível mover a regra padrão.

    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.

11. Conforme necessário, clique no ícone de exclusão ✖para excluir quaisquer regras que você não deseja na política ou selecione **Selecionar regras** para adicionar mais regras.
12. Quando terminar, selecione **Guardar**.

    A página de políticas ILM é atualizada:

    - A política que você salvou é mostrada como proposta. As políticas propostas não têm datas de início e fim.
    - Os botões **Simulate** e **Activate** estão ativados.



13. Vá para "Simulando uma política ILM".

Informações relacionadas

"O que é uma política ILM"

"Gerenciando objetos com o S3 Object Lock"

Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado

Se a configuração global S3 Object Lock estiver ativada, as etapas para criar uma política serão ligeiramente diferentes. Você deve garantir que a política ILM esteja em conformidade com os requisitos de buckets que têm o bloqueio de objeto S3 ativado.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A configuração global de bloqueio de objetos S3D já deve estar ativada para o sistema StorageGRID.

> Se a configuração global S3 Object Lock não tiver sido ativada, use as instruções gerais para criar uma política proposta.
>
> "Criando uma política proposta de ILM"

- Você deve ter criado as regras ILM compatíveis e não compatíveis que 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.

"Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

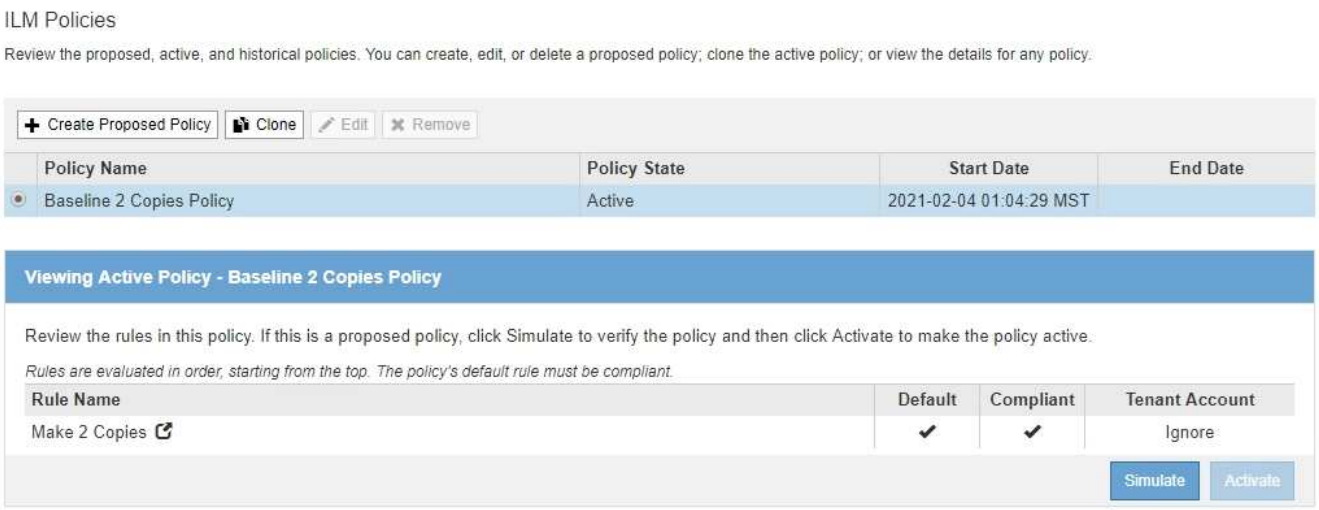
- Você deve ter criado uma regra ILM padrão compatível para a política.

  "Criando uma regra ILM padrão"

Passos

1. Selecione **ILM** > **políticas**.

   É apresentada a página ILM Policies (políticas ILM). Se a configuração Global S3 Object Lock estiver ativada, a página ILM Policies (políticas ILM) indica quais regras ILM são compatíveis.



2. Digite um nome exclusivo para a política proposta no campo **Nome**.

   Você deve inserir pelo menos 1 e não mais de 64 carateres.

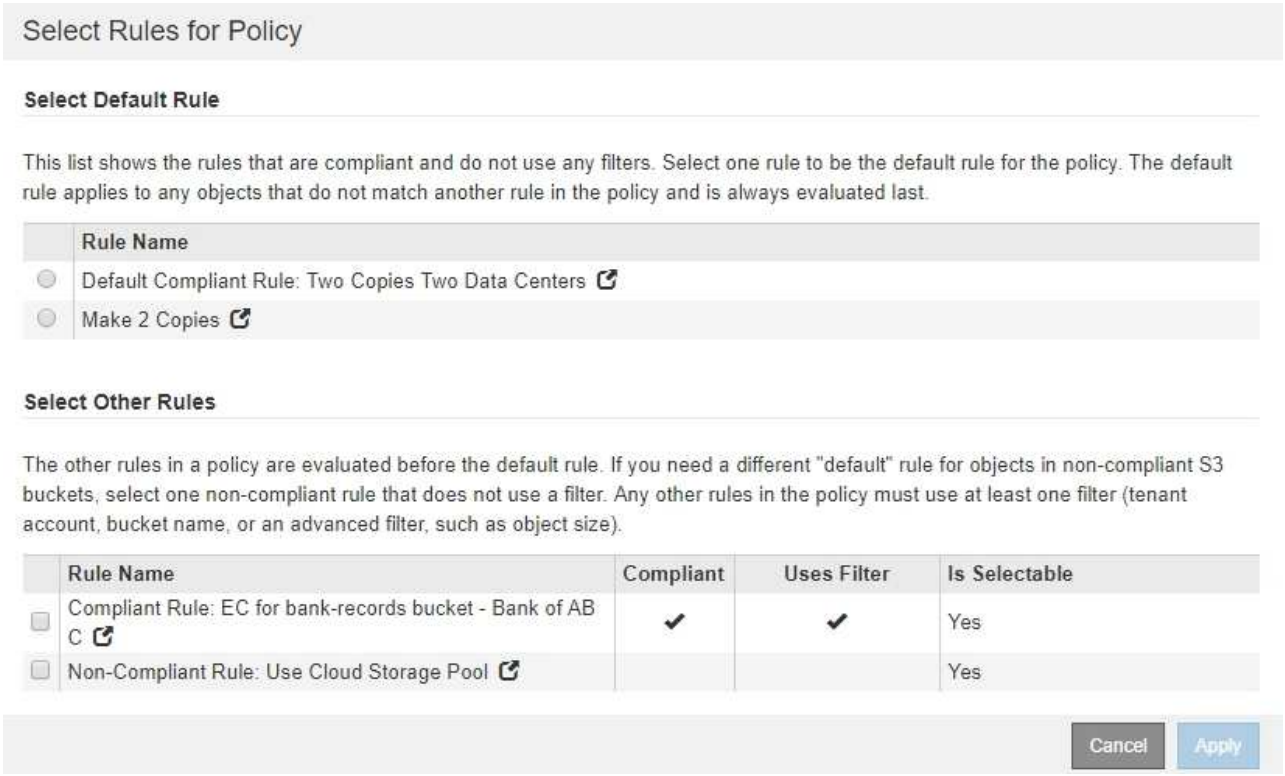
3. Insira o motivo pelo qual você está criando uma nova política proposta no campo **motivo da mudança**.

   Você deve inserir pelo menos 1 e não mais de 128 carateres.

4. Para adicionar regras à política, selecione **Selecionar regras**.

   A caixa de diálogo Selecionar regras para política é exibida, com todas as regras definidas listadas.

   - A seção Selecionar regra padrão lista as regras que podem ser o padrão para uma política compatível. Inclui regras em conformidade que não usam filtros.
   - A seção Selecionar outras regras lista as outras regras compatíveis e não compatíveis que podem ser selecionadas para esta política.



5. Selecione um nome de regra ou o ícone mais detalhes para exibir as configurações dessa regra.
6. Na seção **Selecionar regra padrão**, selecione uma regra padrão para a política proposta.

   A tabela nesta seção lista apenas as regras que são compatíveis e não usam filtros.

   > Se nenhuma regra estiver listada na seção Selecionar regra padrão, você deverá sair da página de política ILM e criar uma regra padrão compatível.
   >
   > "Criando uma regra ILM padrão"

   > Não use a regra fazer 2 cópias de estoque como a 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.

7. Na seção **Selecionar outras regras**, selecione quaisquer outras regras que você deseja incluir na política.

   a. Se você precisar de uma regra diferente de "falha" para objetos em buckets S3 não compatíveis, opcionalmente, selecione uma regra não compatível que não use um filtro.

      Por exemplo, você pode querer usar um pool de armazenamento em nuvem ou um nó de arquivamento 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. Assim que você selecionar uma regra, a coluna **é selecionável** mostra **não** para quaisquer outras regras não compatíveis sem filtros.

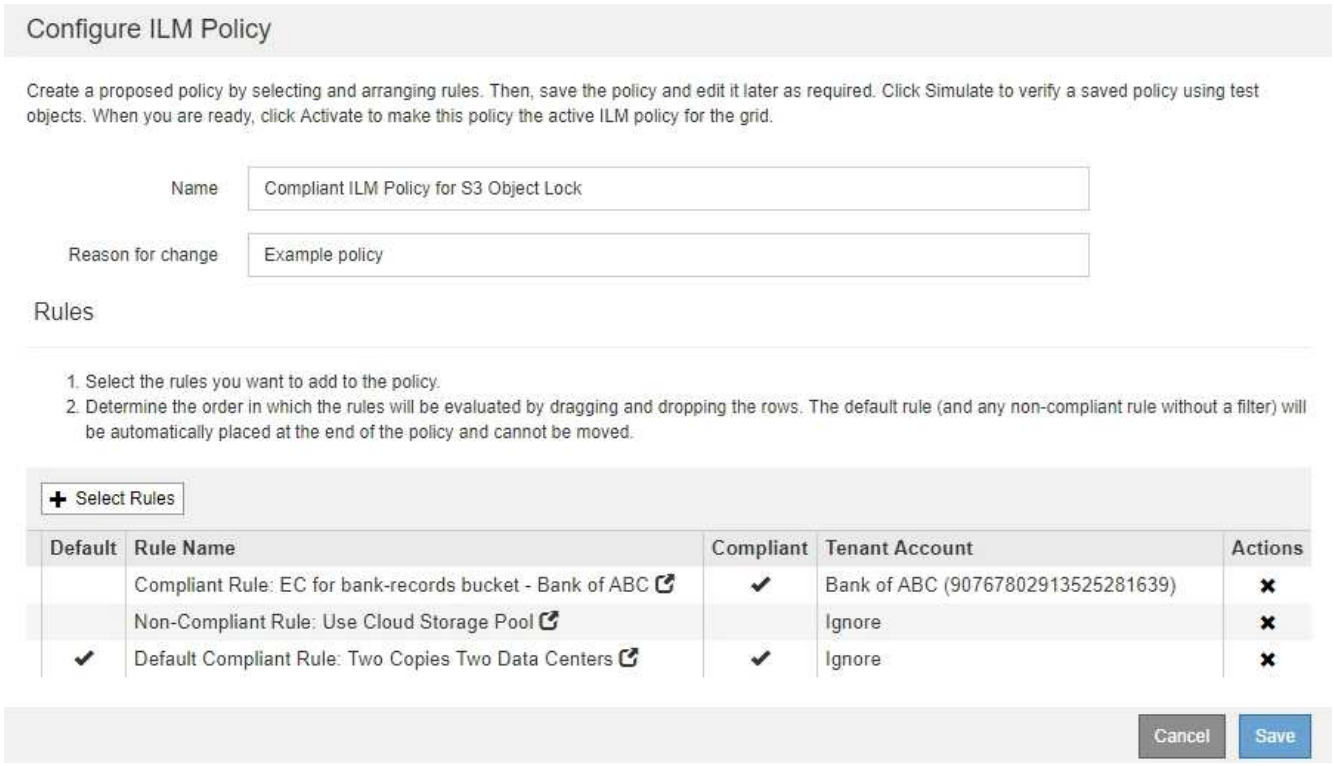
   a. Selecione quaisquer outras regras compatíveis ou não compatíveis que você deseja usar na política.

As outras regras devem usar pelo menos um filtro (conta de locatário, nome do bucket ou um filtro avançado, como tamanho do objeto).

8. Quando terminar de selecionar as regras, selecione **aplicar**.

   As regras selecionadas são listadas. A regra padrão está no final, com as outras regras acima dela. Se você também selecionou uma regra "falha" não compatível, essa regra será adicionada como regra segunda a última na política.

   Neste exemplo, a última regra, 2 cópias 2 Data Centers, é a regra padrão: Ela é compatível e não tem filtros. A regra segunda a última, Cloud Storage Pool, também não tem filtros, mas não é compatível.



   .

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

   Você não pode mover a regra padrão ou a regra "falha" não compatível.

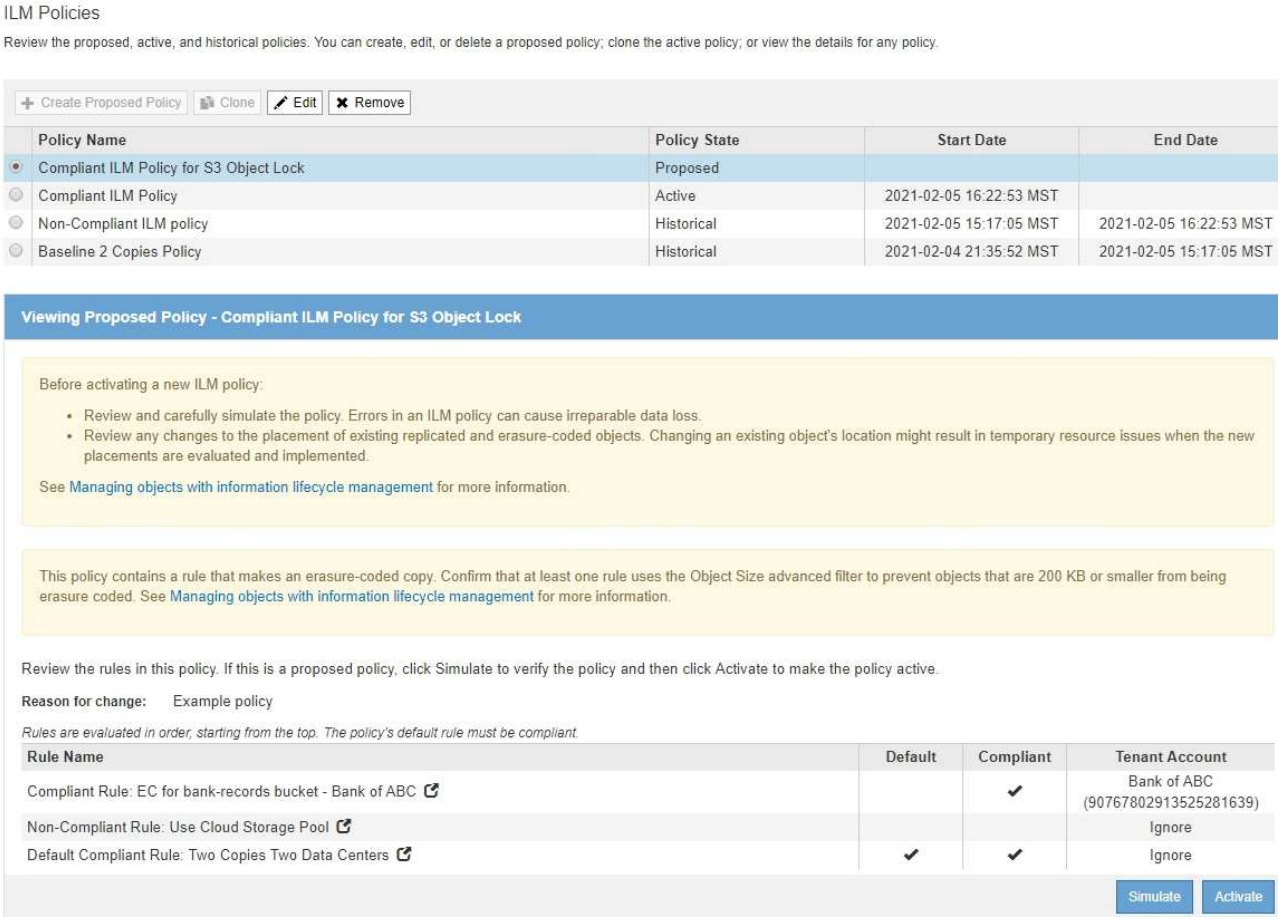
   > Você deve confirmar se as regras ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior.

10. Conforme necessário, clique no ícone de exclusão ✖para excluir quaisquer regras que você não deseja na política ou selecione **Selecionar regras** para adicionar mais regras.
11. Quando terminar, selecione **Guardar**.

    A página de políticas ILM é atualizada:

    - A política que você salvou é mostrada como proposta. As políticas propostas não têm datas de início e fim.

◦ Os botões **Simulate** e **Activate** estão ativados.



12. Vá para "Simulando uma política ILM".

Simulando uma política ILM

Você deve simular 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve saber o bucket/object-key S3 ou o container/object-name Swift para cada objeto que deseja testar e você já deve ter ingerido esses objetos.

Sobre esta tarefa

Você deve selecionar cuidadosamente os objetos que deseja que a política proposta teste. 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. Se a política incluir uma regra padrão para colocar todos os outros objetos, você deve testar pelo menos um objeto de outro intervalo.

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 página Simulação mantém os objetos testados até que você feche, navegue para longe ou atualize a página de políticas ILM.
- Simulação retorna o nome da regra correspondente. Para determinar qual pool de armazenamento ou perfil de codificação de apagamento estão em vigor, você pode exibir o Diagrama de retenção clicando no nome da regra ou no ícone mais detalhes .
- Se o Controle de versão S3 estiver ativado, a política só será simulada em relação à versão atual do objeto.

Passos

1. Selecione e organize as regras e salve a política proposta.

   A política neste exemplo tem três regras:

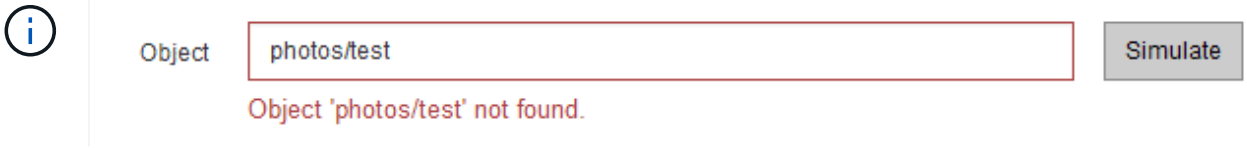
Nome da regra	Filtro	Tipo de cópias	Retenção
X-men	• Inquilino A • Metadados do usuário (série x-man)	2 cópias em dois data centers	2 anos
PNGs	A chave termina com .png	2 cópias em dois data centers	5 anos
Duas cópias de dois data centers	*Nenhum*	2 cópias em dois data centers	Para sempre

2. Clique em **simular**.

É apresentada a caixa de diálogo Simulation ILM Policy (Política ILM de simulação).

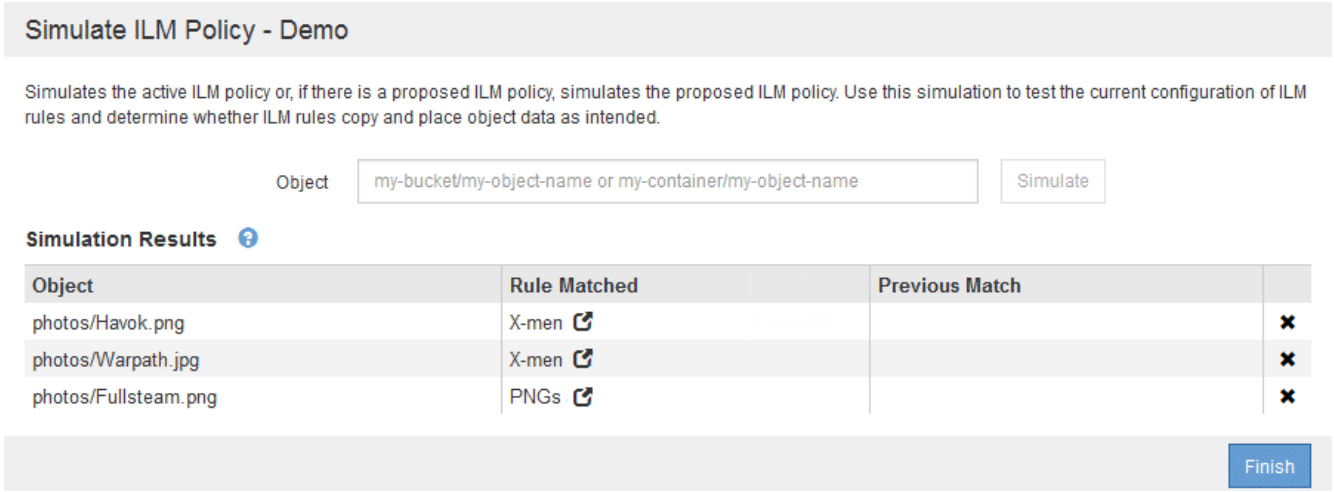
3. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

Uma mensagem será exibida se você especificar um objeto que não foi ingerido.



4. Em **resultados da simulação**, confirme se cada objeto foi correspondido pela regra correta.

No exemplo, os `Havok.png` objetos e `Warpath.jpg` foram corretamente combinados pela regra X-meN. O `Fullsteam.png` objeto, que não inclui `series=x-men` metadados do usuário, não foi correspondido pela regra X-meN, mas foi corretamente correspondido pela regra PNGs. A regra padrão não foi usada porque todos os três objetos foram correspondidos por outras regras.



Exemplos para simular políticas ILM

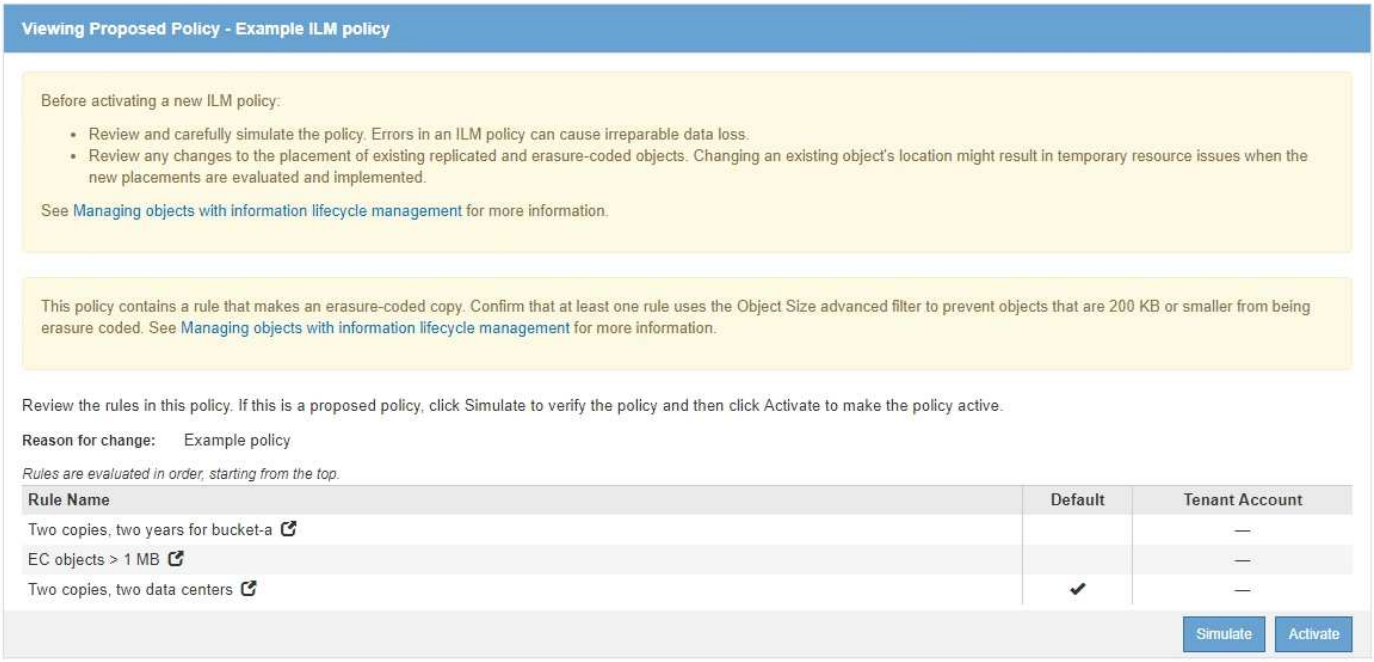
Esses exemplos mostram como você pode verificar regras ILM simulando a política ILM antes de ativá-la.

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

Este exemplo mostra 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 é a regra padrão e não inclui nenhum filtro.



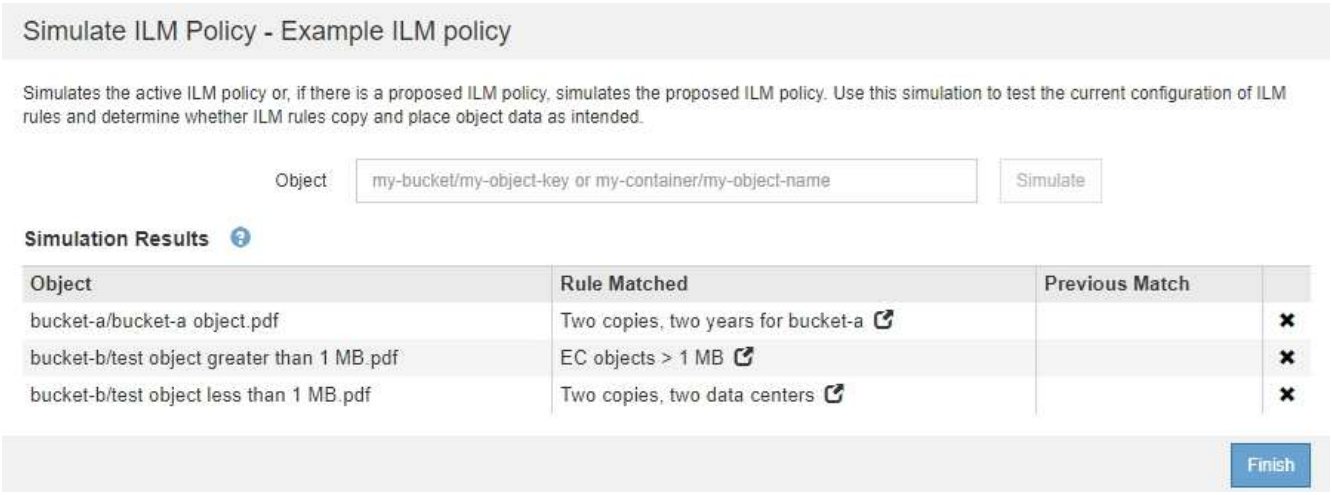
Passos

1. Depois de adicionar as regras e salvar a política, clique em **simular**.

   A caixa de diálogo simular política de ILM é exibida.

2. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

   Os resultados da simulação são exibidos, mostrando qual regra na política corresponde a cada objeto testado.



3. Confirme se cada objeto foi correspondido pela regra correta.

   Neste exemplo:

   a. `bucket-a/bucket-a object.pdf` corresponde corretamente à primeira regra, que filtra os objetos no `bucket-a`.

   b. `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.

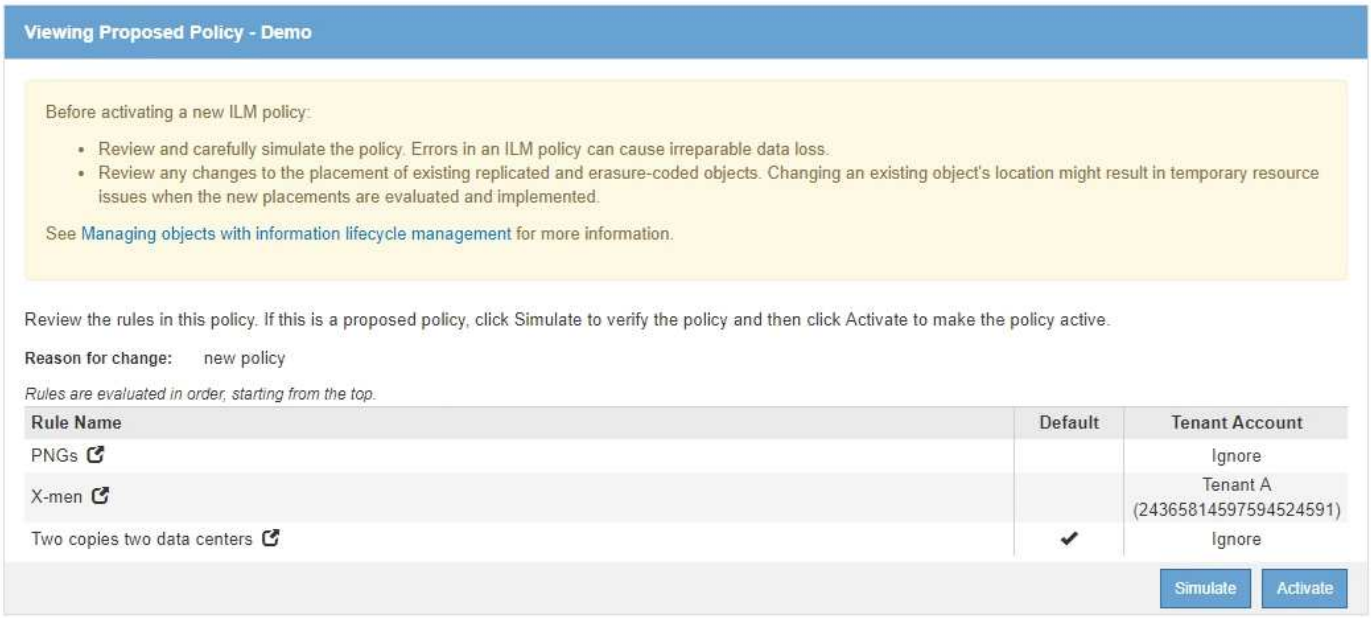
c. `bucket-b/test object less than 1 MB.pdf` não corresponde aos filtros nas duas primeiras regras, por isso será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: Reordenando 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:

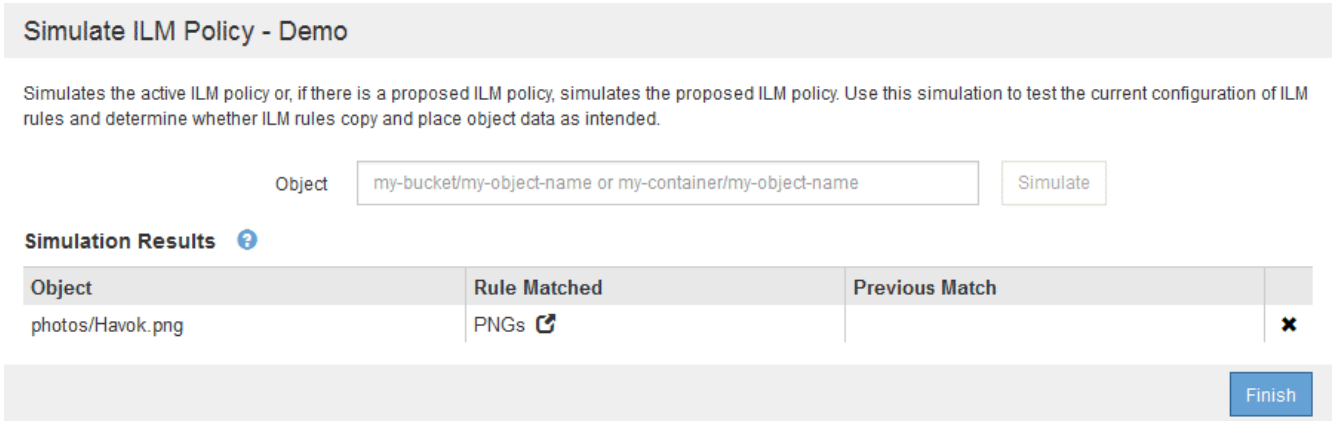
- A primeira regra, **PNGs**, filtra os nomes das chaves que terminam em `.png`.
- A segunda regra, **X-meN**, aplica-se apenas a objetos para o locatário A e filtra os metadados `series=x-men` do usuário.
- A última regra, **duas cópias dois data centers**, é a regra padrão, que corresponde a quaisquer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



Passos

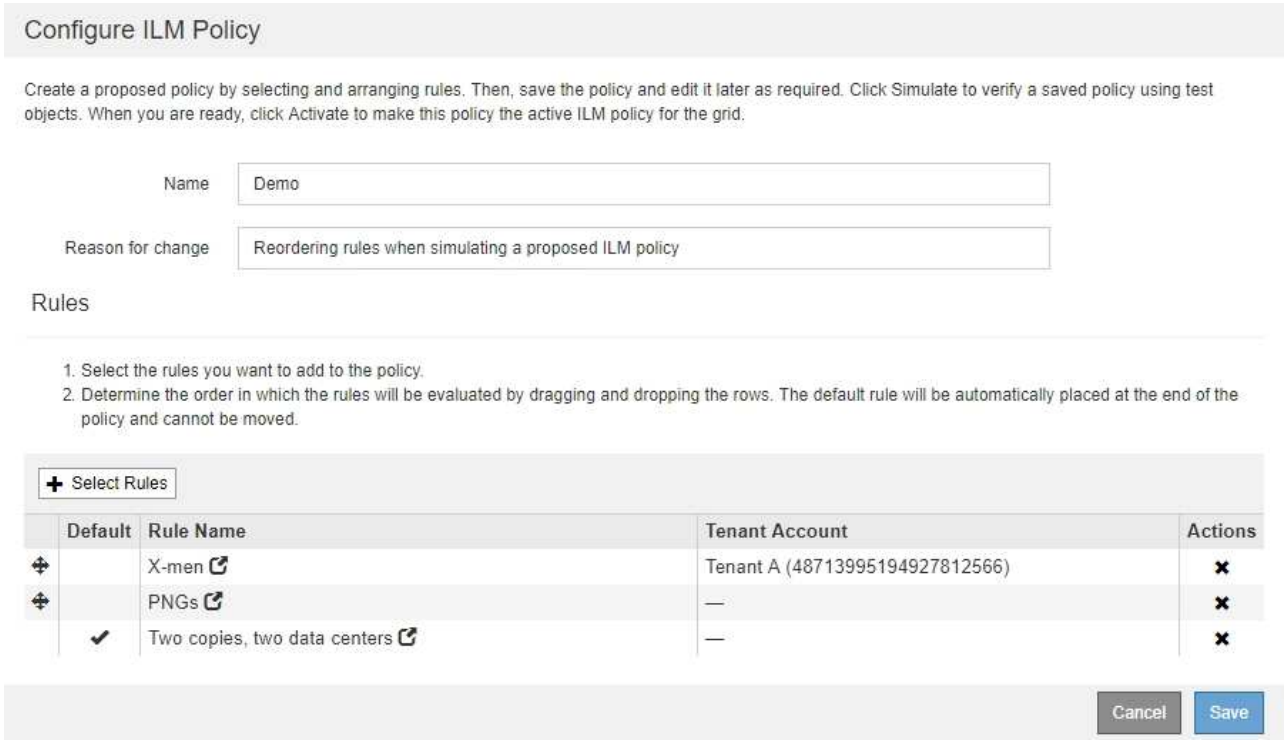
1. Depois de adicionar as regras e salvar a política, clique em **simular**.
2. No campo **Object**, insira o bucket/object-key S3 ou o container/object-name Swift para um objeto de teste e clique em **Simulate**.

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



No entanto, a regra que o `Havok.png` objeto foi destinado a testar foi a regra **X-men**.

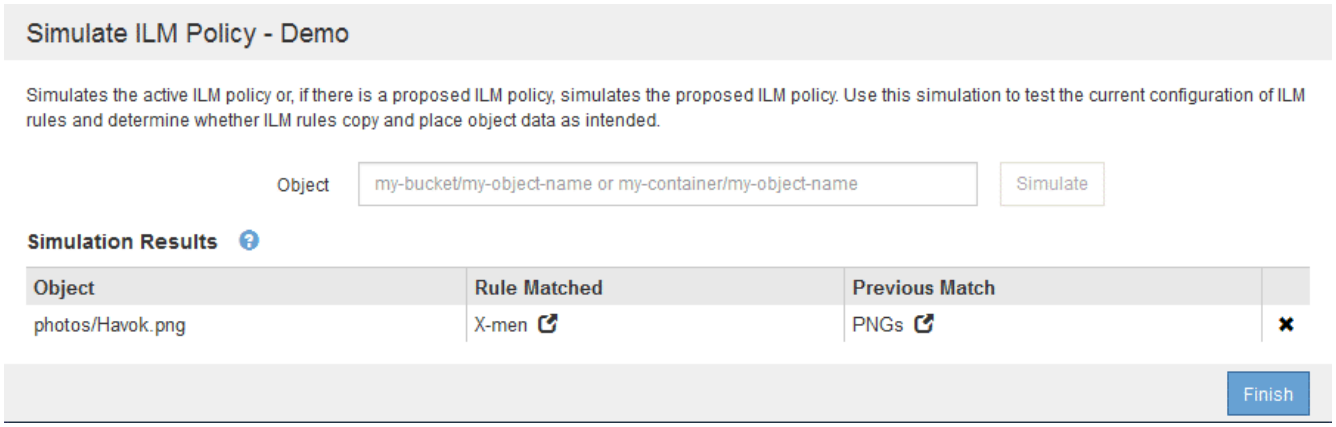
3. Para resolver o problema, reordene as regras.
   a. Clique em **Finish** para fechar a página Simulate ILM Policy.
   b. Clique em **Editar** para editar a política.
   c. Arraste a regra **X-man** para o topo da lista.



   d. Clique em **Salvar**.

4. Clique em **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.

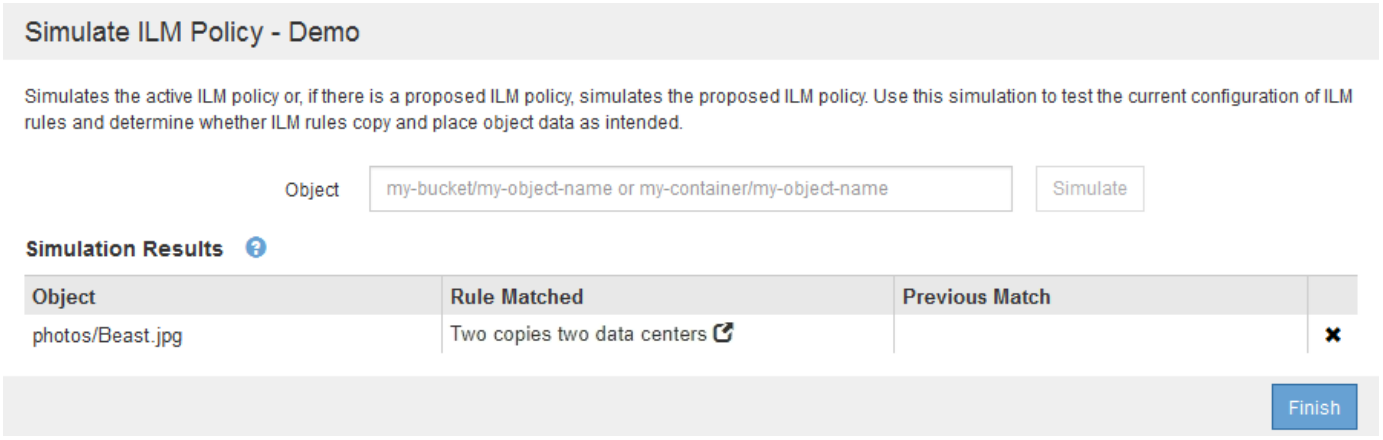


Se você permanecer na página Configurar políticas, poderá simular novamente uma política depois de fazer alterações sem precisar digitar novamente os nomes dos objetos de teste.

Exemplo 3: Corrigindo 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.

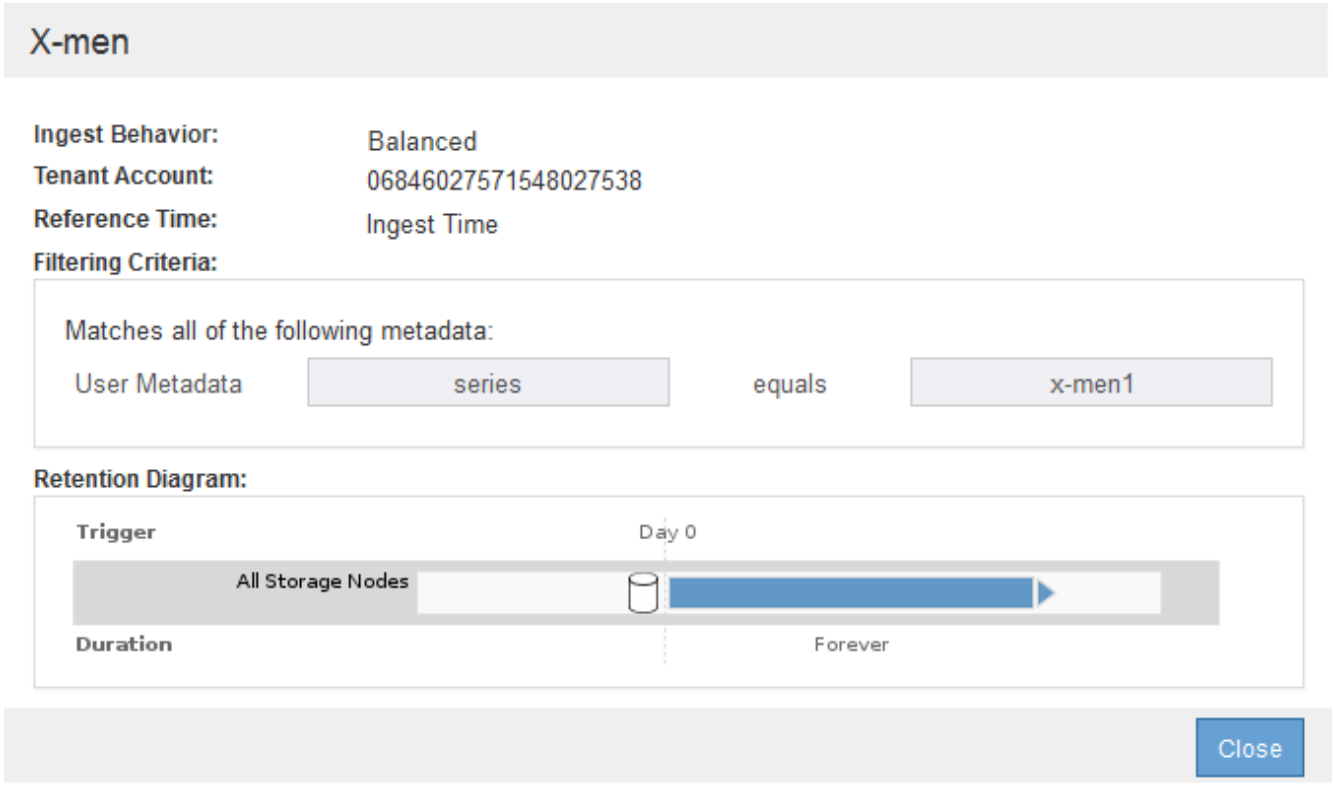


Quando um objeto de teste não é correspondido pela regra esperada na política, você deve examinar cada regra na política e corrigir quaisquer erros.

Passos

1. Para cada regra na política, exiba as configurações da regra clicando no nome da regra ou no ícone mais detalhes em qualquer caixa de diálogo em que a regra é exibida.
2. Revise a conta de locatário da regra, o tempo de referência e os critérios de filtragem.

   Neste exemplo, os metadados da regra X-meN incluem um erro. O valor dos metadados foi inserido como "'x-men1" 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.

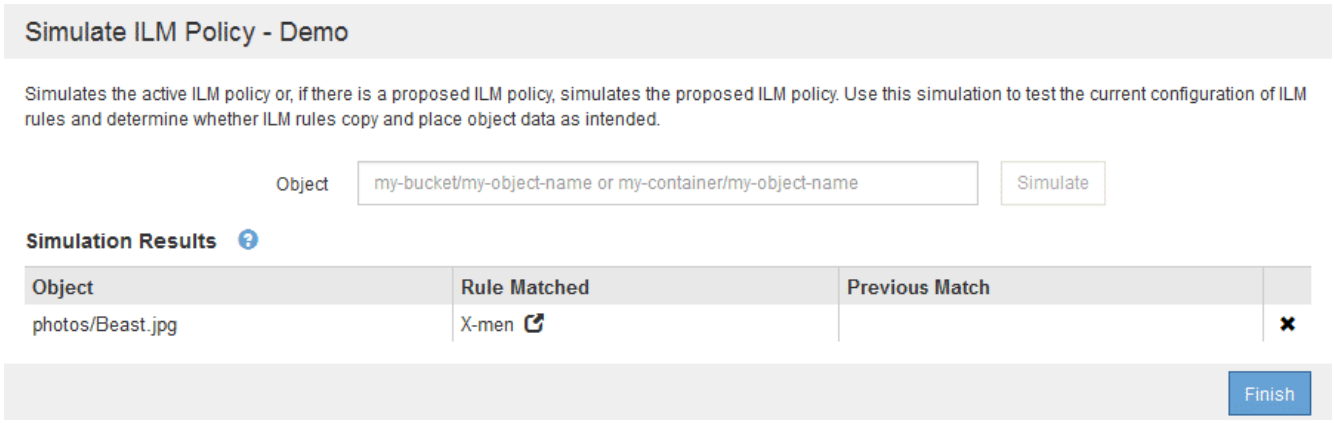
Opção	Descrição
Clonar a regra	i. Selecione **ILM** > **regras**. ii. Selecione a regra incorreta e clique em **Clone**. iii. Altere as informações incorretas e clique em **Salvar**. iv. Selecione **ILM** > **políticas**. v. Selecione a política proposta e clique em **Editar**. vi. Clique em **Selecionar regras**. vii. Marque a caixa de seleção da nova regra, desmarque a caixa de seleção da regra original e clique em **aplicar**. viii. Clique em **Salvar**.

Opção	Descrição
Editando a regra	i. Selecione a política proposta e clique em **Editar**. ii. Clique no ícone de exclusão ✖para remover a regra incorreta e clique em **Salvar**. iii. Selecione **ILM** > **regras**. iv. Selecione a regra incorreta e clique em **Editar**. v. Altere as informações incorretas e clique em **Salvar**. vi. Selecione **ILM** > **políticas**. vii. Selecione a política proposta e clique em **Editar**. viii. Selecione a regra corrigida, clique em **Apply** e clique em **Save**.

4. Execute a simulação novamente.

> ⓘ Como você navegou para fora da página de políticas ILM para editar a regra, os objetos que você inseriu anteriormente para simulação não são mais exibidos. Você deve digitar novamente os nomes dos objetos.

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



Ativar 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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Tem de ter guardado e simulado 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

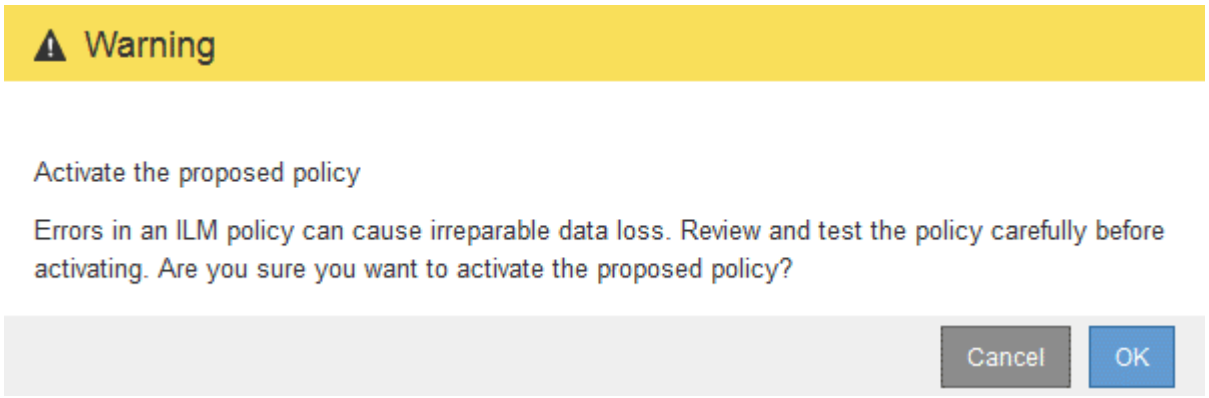
Quando você ativa uma política de ILM, o sistema distribui a nova política para todos os nós. No entanto, a nova política ativa pode não ter efeito até que todos os nós de grade estejam disponíveis para receber a nova política. Em alguns casos, o sistema espera implementar uma nova política ativa para 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 será marcada como ""ativa"", mas ela não entrará em vigor até que todos os nós estejam online e disponíveis.

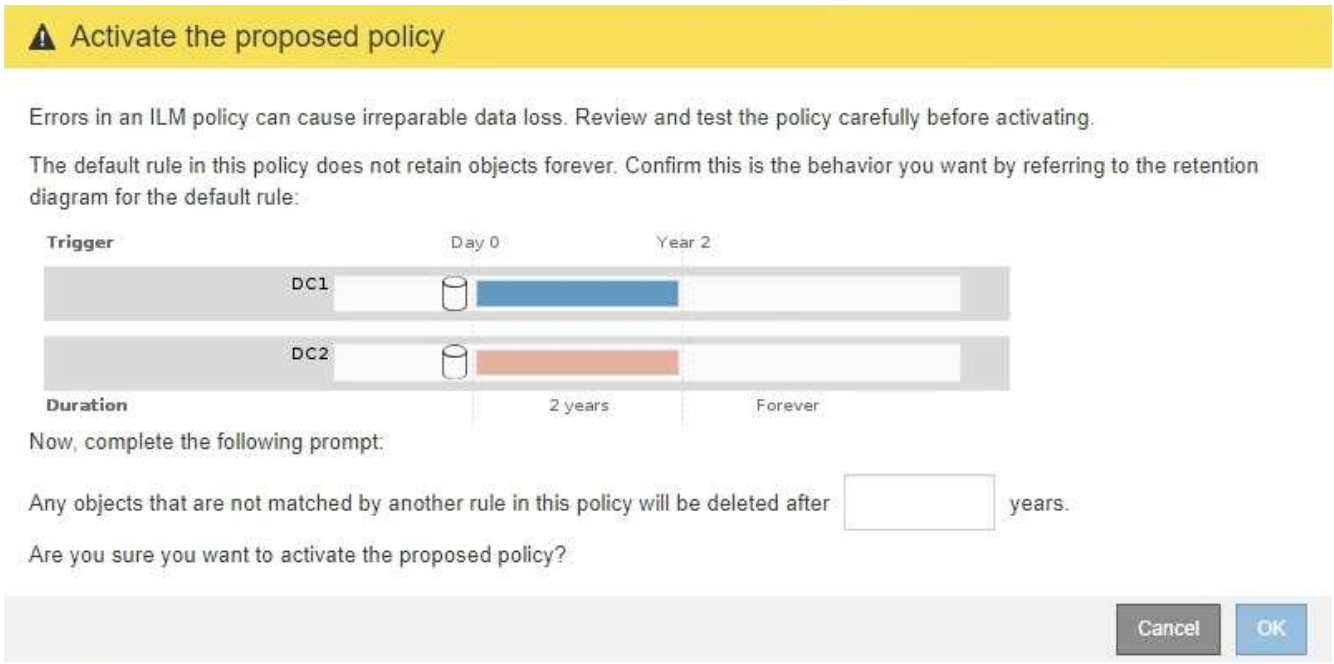
Passos

1. Quando estiver pronto para ativar uma política proposta, selecione a política na página políticas ILM e clique em **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 da política não retiver objetos para sempre. Neste exemplo, o diagrama de retenção mostra que a regra padrão excluirá objetos após 2 anos. Você deve digitar **2** na caixa de texto para confirmar que quaisquer objetos não correlacionados por outra regra na política serão removidos do StorageGRID após 2 anos.

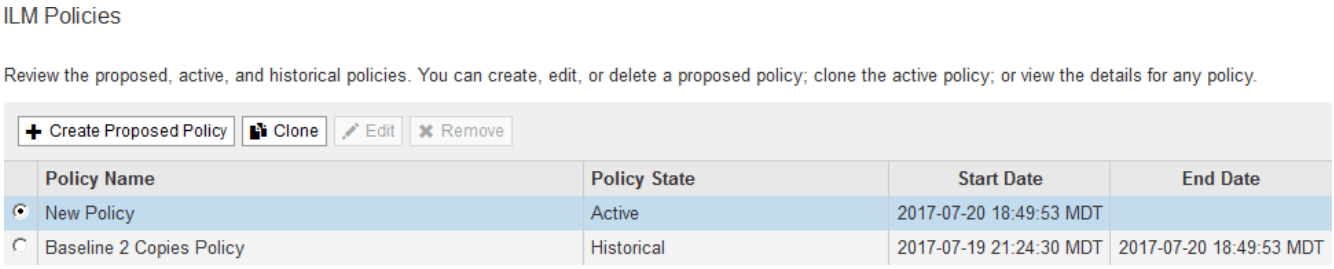


2. Clique em **OK**.

Resultado

Quando uma nova política ILM tiver sido ativada:

- A política é mostrada com um estado de política ativo na tabela na página políticas de ILM. A entrada Data Início indica a data e a hora em que a política foi ativada.



- A política anteriormente ativa é mostrada com um Estado Histórico da Política. As entradas 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"

Verificando 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.

O que você vai precisar

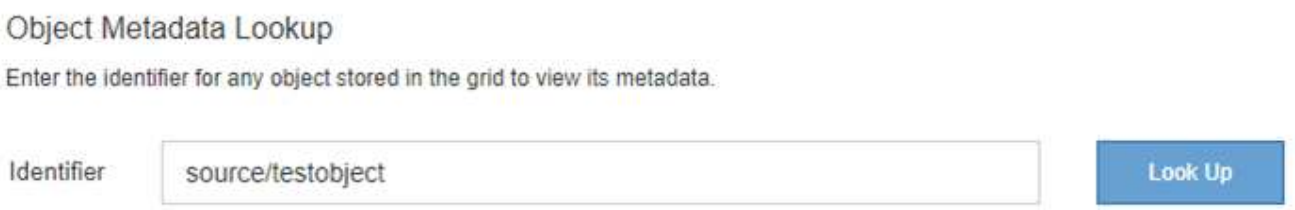
- Você deve ter um identificador de objeto, que pode ser um dos seguintes:
  - **UUID**: O Identificador universalmente exclusivo do objeto. Introduza o UUID em todas as maiúsculas.

- **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.
- * 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. Ingira 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. Clique em **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": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


5. 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, consulte as informações sobre como entender as mensagens de auditoria.

Informações relacionadas

"Rever registos de auditoria"

"Use S3"

"Use Swift"

Trabalhando com regras de ILM e políticas de ILM

Depois de criar regras ILM e uma política ILM, você poderá continuar trabalhando com elas, modificando sua configuração à medida que seus requisitos de storage mudarem.

Excluindo uma regra ILM

Para manter a lista de regras atuais do ILM gerenciável, exclua quaisquer regras do ILM que você provavelmente não usará.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

> Não é possível excluir uma regra ILM se ela for usada atualmente na política ativa ou na política proposta. Se você precisar excluir uma regra ILM que é usada em uma política, execute estas etapas primeiro:
>
> 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.

Passos

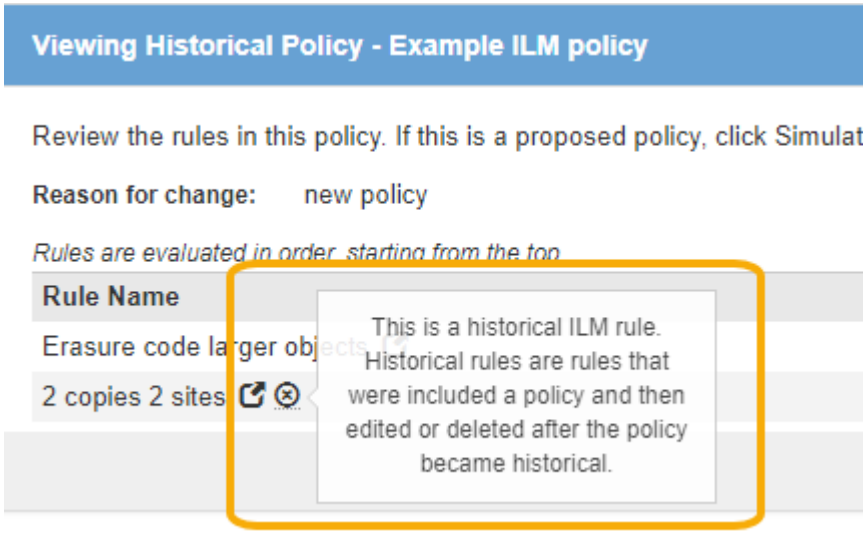
1. Selecione **ILM** > **regras**.
2. Revise a entrada da tabela para a regra que deseja remover.

   Confirme se a regra não é usada na política ILM ativa ou na política ILM proposta.

3. Se a regra que você deseja remover não estiver em uso, selecione o botão de opção e selecione **Remover**.
4. Selecione **OK** para confirmar que deseja excluir a regra ILM.

   A regra ILM é excluída.

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



Informações relacionadas

"Criando uma política ILM"

Editar uma regra ILM

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

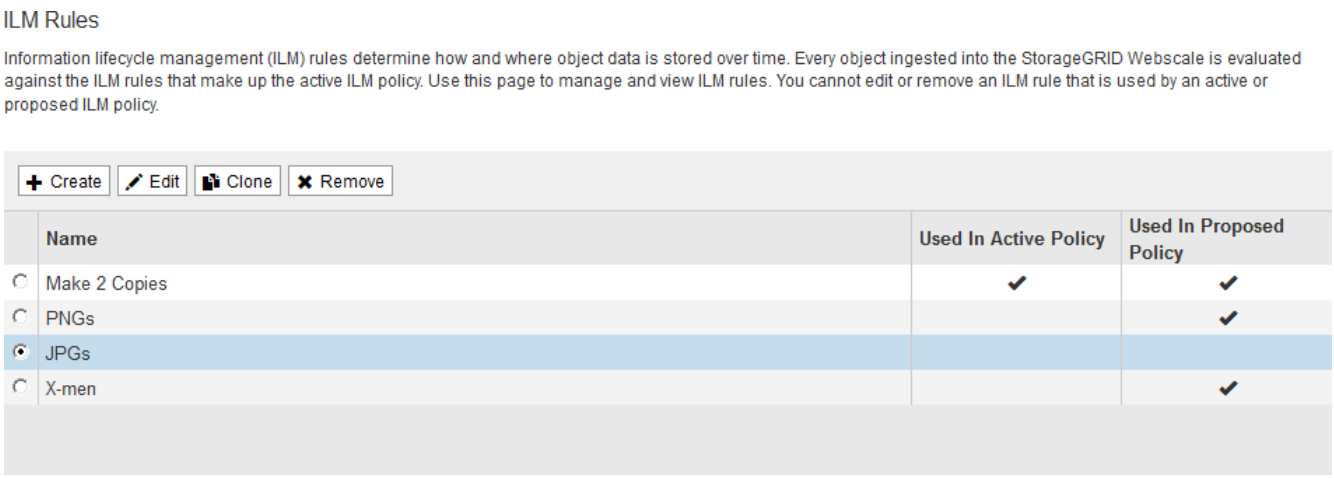
Não é possível editar uma regra se ela estiver sendo usada na política ILM proposta ou na política ILM ativa. Em vez disso, você pode clonar essas regras e fazer as alterações necessárias na cópia clonada. Você também não pode editar a regra ILM de estoque (fazer 2 cópias) ou regras ILM criadas antes da versão 10,3 do StorageGRID.

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**.

   A página regras do ILM é exibida. Esta página mostra todas as regras disponíveis e indica quais regras estão sendo usadas na política ativa ou na política proposta.



2. Selecione uma regra que não esteja sendo usada e clique em **Editar**.

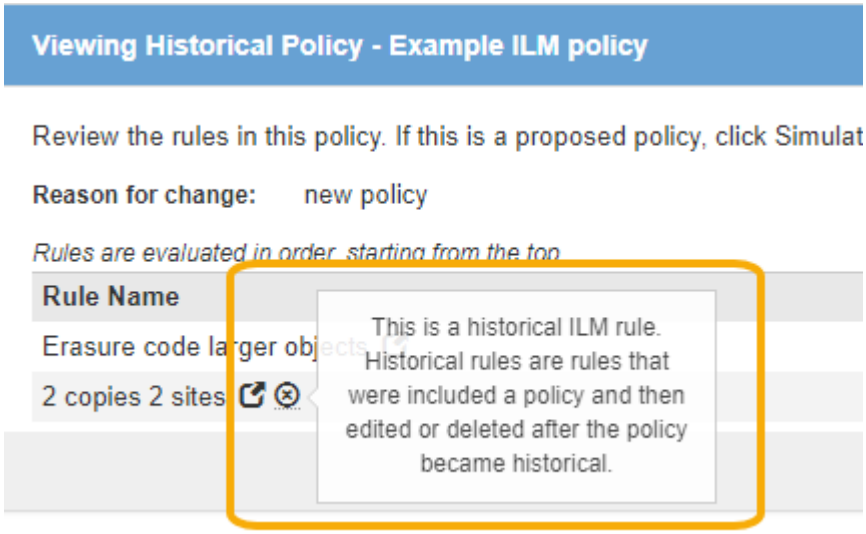
   O assistente Editar regra ILM é aberto.

3. Complete as páginas do assistente Editar regra ILM, seguindo as etapas para criar uma regra ILM e usar filtros avançados, conforme necessário.

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

4. Clique em **Salvar**.

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



Informações relacionadas

"Criando uma regra ILM"

"Usando filtros avançados em regras ILM"

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.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

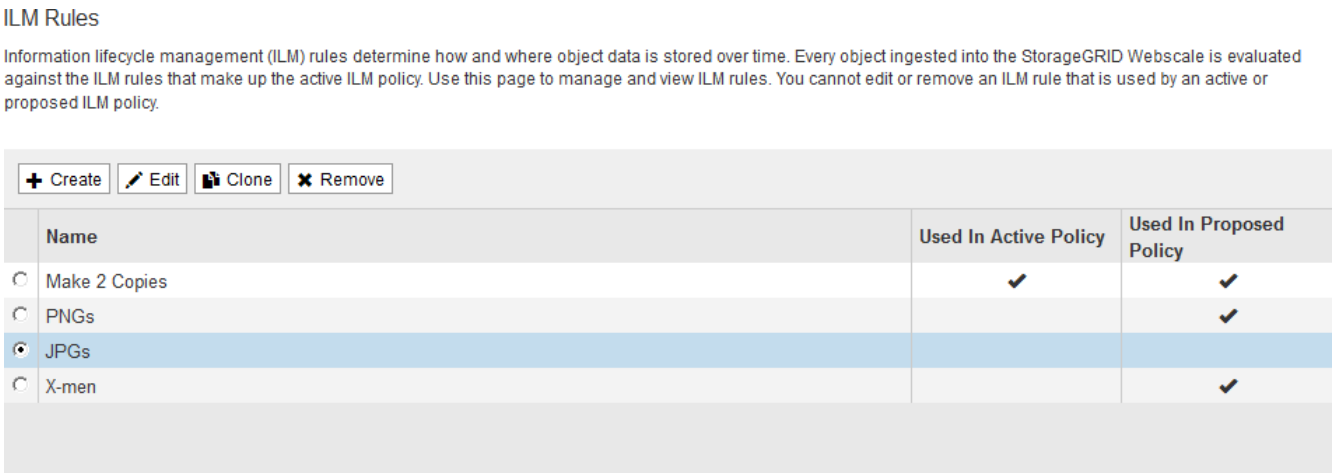
Sobre esta tarefa

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**.

   A página regras do ILM é exibida.



2. Selecione a regra ILM que deseja clonar e clique em **Clone**.

   O assistente criar regra ILM é aberto.

3. Atualize a regra clonada seguindo as etapas para editar uma regra ILM e usando filtros avançados.

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

4. Clique em **Salvar**.

   A nova regra ILM é criada.

Informações relacionadas

"Trabalhando com regras de ILM e políticas de ILM"

"Usando filtros avançados em regras ILM"

Visualizar a fila de atividades da política ILM

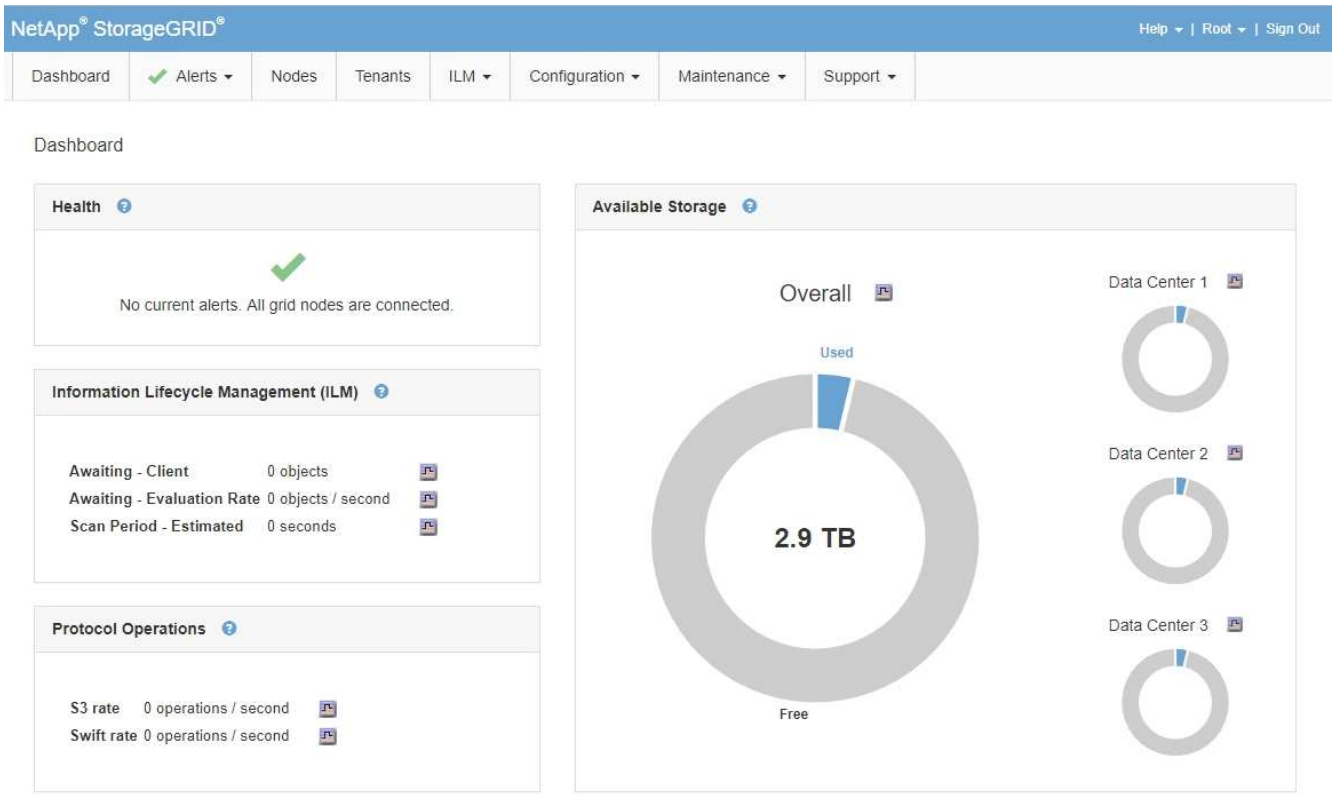
Você pode exibir o número de objetos que estão na fila a serem avaliados em relação à política ILM a qualquer momento. Você pode querer monitorar a fila de processamento ILM para determinar o desempenho do sistema. Uma fila grande pode indicar que o sistema não é capaz de acompanhar a taxa de ingestão, a carga dos aplicativos cliente é muito grande ou que existe alguma condição anormal.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Painel**.



2. Monitore a seção Gerenciamento do ciclo de vida das informações (ILM).

   Você pode clicar no ponto de interrogação para ver uma descrição dos itens nesta seção.

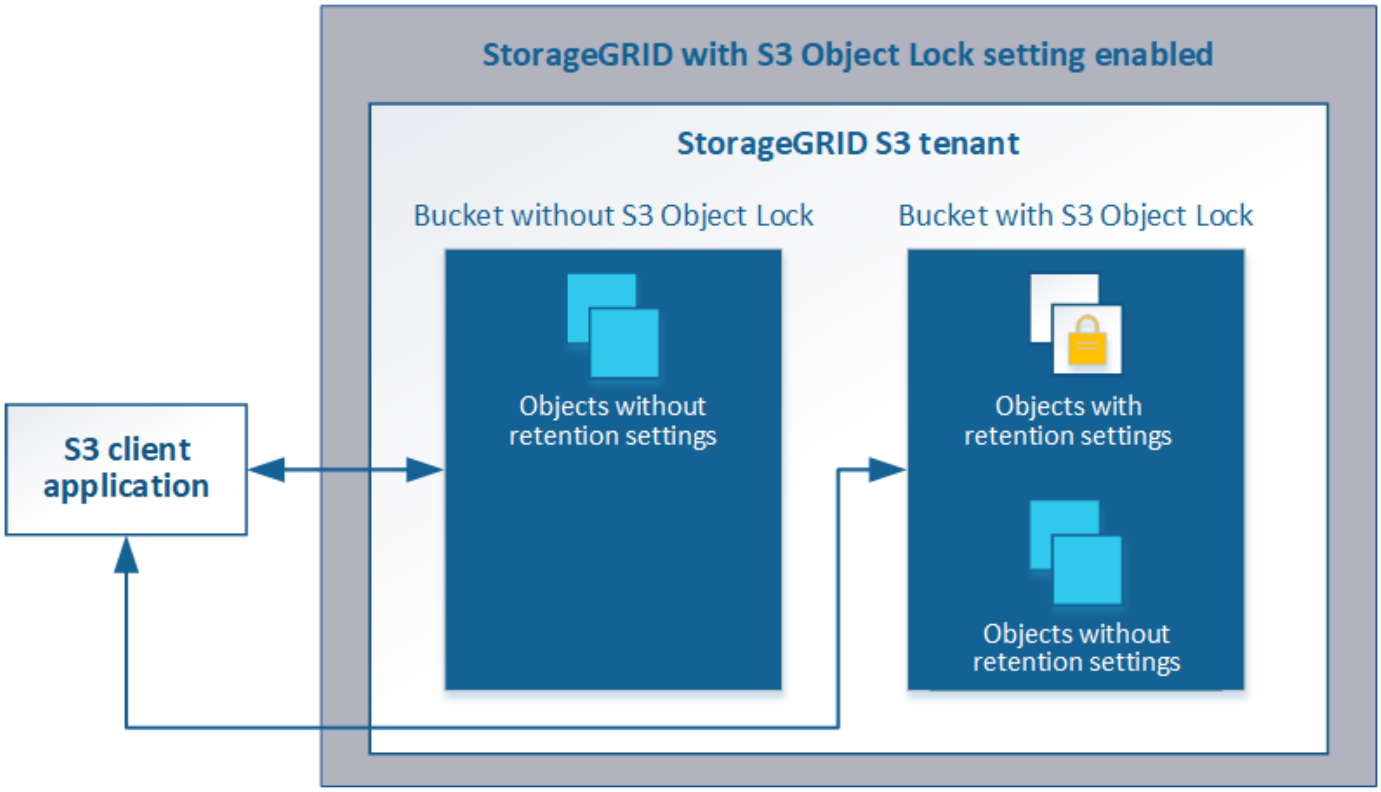
Gerenciando objetos com o S3 Object Lock

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

O que é S3 Object Lock?

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

Como mostrado na figura, quando a configuração global de bloqueio de objeto S3D está ativada para um sistema StorageGRID, uma conta de locatário S3D pode criar buckets com ou sem bloqueio de objeto S3D ativado. Se um bucket tiver o bloqueio de objeto S3 ativado, os aplicativos cliente S3 podem, opcionalmente, especificar configurações de retenção para qualquer versão de objeto nesse bucket. Uma versão de objeto deve ter configurações de retenção especificadas para ser protegida pelo bloqueio de objeto S3.



O recurso bloqueio de objetos do StorageGRID S3 fornece um modo de retenção único equivalente ao modo de conformidade do Amazon S3. Por padrão, uma versão de objeto protegido não pode ser substituída ou excluída por nenhum usuário. O recurso bloqueio de objetos do StorageGRID S3 não suporta um modo de governança e não permite que usuários com permissões especiais ignorem as configurações de retenção ou excluam objetos protegidos.

Se um bucket tiver o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar uma ou ambas as seguintes configurações de retenção no nível do objeto ao criar ou atualizar um objeto:

- **Retent-until-date**: Se a data de retent-until de uma versão de objeto for no futuro, o objeto pode ser recuperado, mas não pode ser modificado ou excluído. Conforme necessário, a data de retenção até um objeto pode ser aumentada, mas essa data não pode ser diminuída.
- **Retenção legal**: Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar colocar uma retenção legal em um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até que seja explicitamente removida. As obrigações legais são independentes da retenção até à data.

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

Comparação do S3 Object Lock com a conformidade legada

O recurso bloqueio de objetos S3 no StorageGRID 11,5 substitui o recurso de conformidade que estava disponível nas versões anteriores do StorageGRID. Como o novo recurso de bloqueio de objetos do S3 está em conformidade com os requisitos do Amazon S3, ele deprecia o recurso proprietário de conformidade do StorageGRID, que agora é conhecido como ""conformidade legada"".

Se você ativou anteriormente a configuração de conformidade global, a nova configuração global de bloqueio

de objetos S3 será ativada automaticamente quando você atualizar para o StorageGRID 11,5. Os usuários do locatário não poderão mais criar novos buckets com a conformidade habilitada no StorageGRID 11,5. No entanto, conforme necessário, os usuários do locatário podem continuar a usar e gerenciar quaisquer buckets em conformidade legados existentes, incluindo a realização das seguintes tarefas:

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

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

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

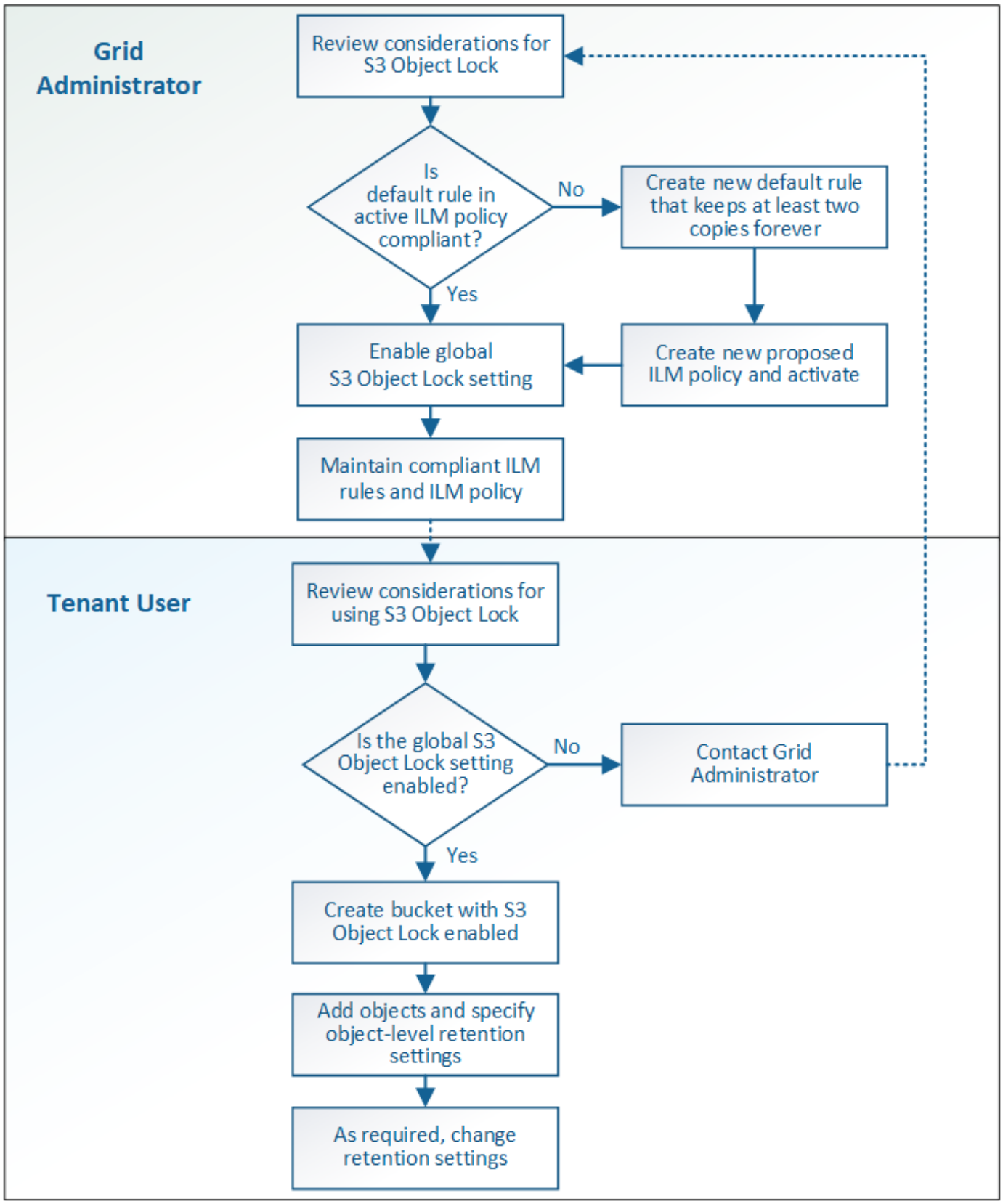
	S3 bloqueio de objetos (novo)	**Conformidade (legado)**
Como o recurso é ativado globalmente?	No Gerenciador de Grade, selecione **Configuração** > **Configurações do sistema** > **bloqueio de objetos S3**.	Já não é suportado. **Observação:** se você ativou previamente a configuração de conformidade global, a configuração global de bloqueio de objetos S3 será ativada automaticamente quando você atualizar para o StorageGRID 11,5.
Como o recurso está habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto S3 ao criar um novo bucket usando o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3.	Os usuários não podem mais criar novos buckets com a conformidade ativada. No entanto, eles podem continuar adicionando novos objetos aos buckets em conformidade existentes.
O controle de versão do bucket é suportado?	Sim. O controle de versão do bucket é necessário e é ativado automaticamente quando o bloqueio de objetos S3 é ativado para o bucket.	Não. O recurso de conformidade legado não permite o controle de versão do bucket.
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção até cada versão do objeto.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção aplica-se a todos os objetos no balde.

	S3 bloqueio de objetos (novo)	Conformidade (legado)
Um bucket pode ter configurações padrão para retenção e retenção legal?	Não. Os buckets StorageGRID que têm o bloqueio de objeto S3 ativado não têm um período de retenção predefinido. Em vez disso, você pode especificar uma data de retenção até cada versão do objeto.	Sim
O período de retenção pode ser alterado?	A data de retenção até uma versão de objeto pode ser aumentada, mas nunca diminuída.	O período de retenção do balde pode ser aumentado, mas nunca diminuído.
Onde é controlada a guarda legal?	Os usuários podem colocar uma retenção legal ou levantar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no balde e afeta todos os objetos no balde.
Quando os objetos podem ser excluídos?	Uma versão de objeto pode ser excluída após a data de retenção ser alcançada, assumindo que o objeto não está sob retenção legal.	Um objeto pode ser excluído após o período de retenção expirar, supondo que o intervalo não esteja sob retenção legal. Os objetos podem ser excluídos automaticamente ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

Fluxo de trabalho para S3 Object Lock

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

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



Tarefas de administração de grade

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

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

Tarefas do usuário do locatário

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

1. Crie buckets que tenham o bloqueio de objeto S3 ativado.
2. Adicione objetos a esses buckets e especifique períodos de retenção no nível do objeto e configurações de retenção legal.
3. Conforme necessário, atualize um período de retenção ou altere a configuração de retenção legal para um objeto individual.

Informações relacionadas

"Use uma conta de locatário"

"Use S3"

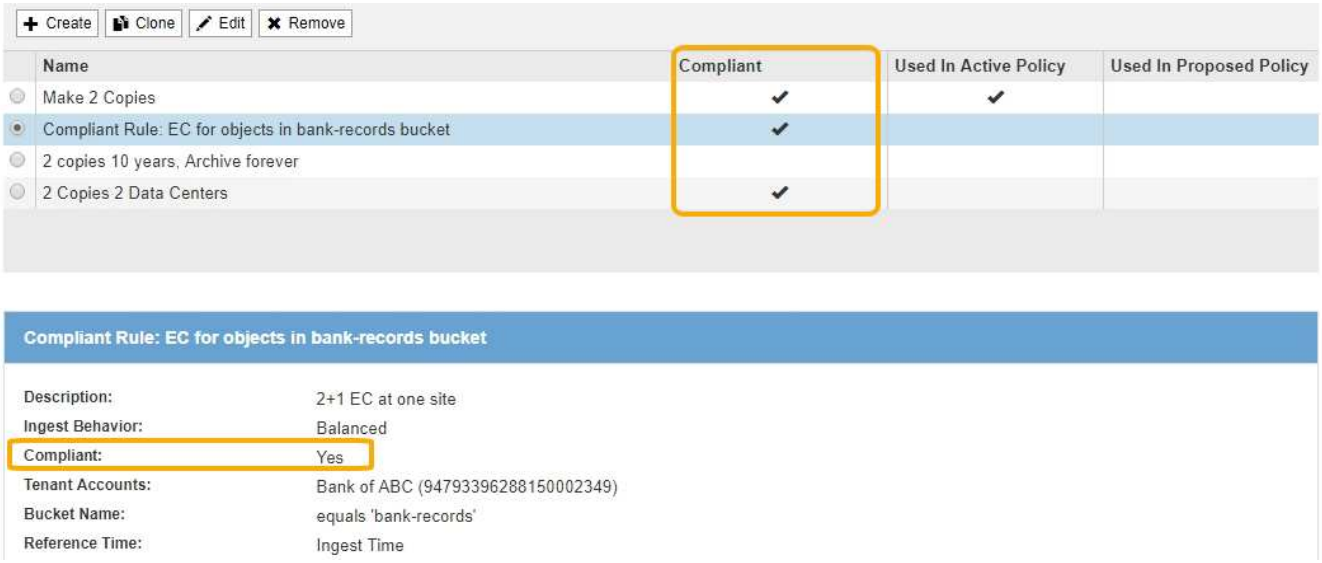
Requisitos para o bloqueio de objetos S3

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

Requisitos para usar a configuração global S3 Object Lock

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

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

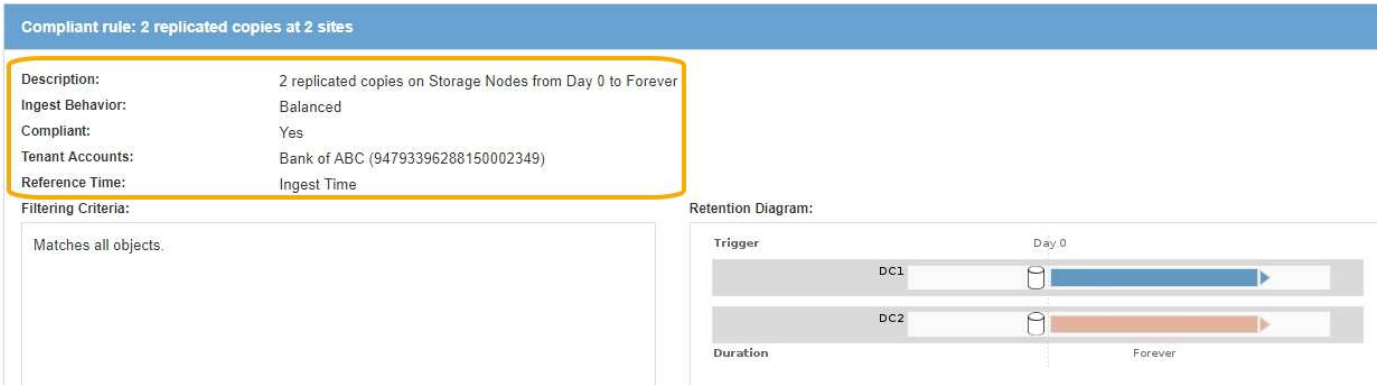


Requisitos para regras ILM compatíveis

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

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

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



Requisitos para políticas de ILM ativas e propostas

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

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

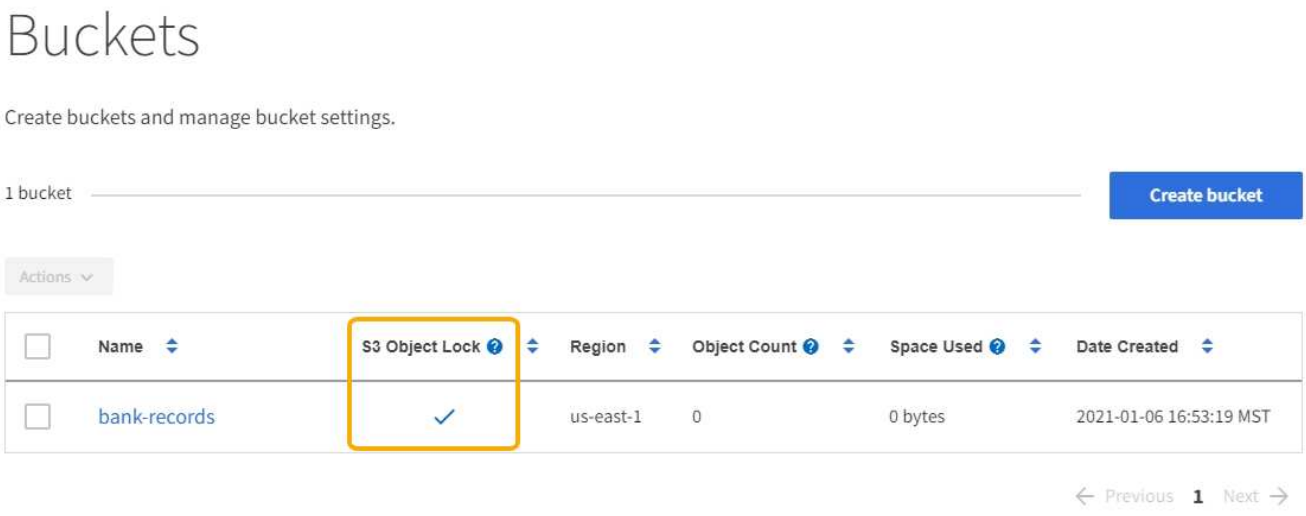
Uma política de ILM compatível pode incluir estas três regras:

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

Requisitos para buckets com bloqueio de objeto S3 ativado

- Se a configuração global de bloqueio de objeto S3 estiver ativada para o sistema StorageGRID, você poderá usar o Gerenciador de locatário, a API de gerenciamento de locatário ou a API REST S3 para criar buckets com o bloqueio de objeto S3 ativado.

  Este exemplo do Gerenciador do Locatário mostra um bucket com o bloqueio de objeto S3 ativado.



- Se você planeja usar o bloqueio de objetos S3D, você deve ativar o bloqueio de objetos S3D ao criar o bucket. Não é possível ativar o bloqueio de objetos S3D para um bucket existente.
- O controle de versão do bucket é necessário com o S3 Object Lock. Quando o bloqueio de objeto S3 está ativado para um bucket, o StorageGRID ativa automaticamente o controle de versão desse bucket.
- Depois de criar um bucket com o bloqueio de objetos S3 ativado, não é possível desativar o bloqueio de objetos S3 ou suspender o controle de versão desse bucket.
- Um bucket do StorageGRID que tenha o bloqueio de objetos S3 ativado não tem um período de retenção padrão. Em vez disso, o aplicativo cliente S3 pode, opcionalmente, especificar uma data de retenção e

uma configuração de retenção legal para cada versão de objeto adicionada a esse bucket.

- A configuração do ciclo de vida do bucket é compatível com buckets do ciclo de vida do objeto do S3.
- A replicação do CloudMirror não é compatível com buckets com o S3 Object Lock ativado.

Requisitos para objetos em buckets com o bloqueio de objetos S3 ativado

- O aplicativo cliente S3 deve especificar configurações de retenção para cada objeto que precisa ser protegido pelo bloqueio de objetos S3.
- Você pode aumentar a data de retenção até uma versão de objeto, mas nunca pode diminuir esse valor.
- Se você for notificado de uma ação legal pendente ou investigação regulatória, poderá preservar informações relevantes colocando uma retenção legal em uma versão de objeto. Quando uma versão de objeto está sob uma retenção legal, esse objeto não pode ser excluído do StorageGRID, mesmo que tenha atingido sua data de retenção até. Assim que a retenção legal for levantada, a versão do objeto pode ser excluída se a data de retenção for atingida.
- S3 Object Lock requer o uso de buckets versionados. As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção de data e de retenção legal, uma mas não a outra, ou nenhuma. Especificar uma configuração reter-até-data ou retenção legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida dos objetos em buckets com o bloqueio de objetos S3 ativado

Cada objeto que é salvo em um bucket com o S3 Object Lock ativado passa por três estágios:

1. * Ingestão de objetos*
   - Ao adicionar uma versão de objeto a um bucket com o bloqueio de objeto S3 ativado, o aplicativo cliente S3 pode, opcionalmente, especificar configurações de retenção para o objeto (reter até a data, retenção legal ou ambos). Em seguida, o StorageGRID gera metadados para esse objeto, que inclui um identificador de objeto exclusivo (UUID) e a data e hora de ingestão.
   - Depois que uma versão de objeto com configurações de retenção é ingerida, seus dados e metadados S3 definidos pelo usuário não podem ser modificados.
   - O StorageGRID armazena os metadados do objeto independentemente dos dados do objeto. Ele mantém três cópias de todos os metadados de objetos em cada local.
2. **Retenção de objetos**
   - Várias cópias do objeto são armazenadas pelo StorageGRID. O número exato e o tipo de cópias e os locais de storage são determinados pelas regras em conformidade na política de ILM ativa.
3. **Exclusão de objeto**
   - Um objeto pode ser excluído quando sua data de retenção é alcançada.
   - Não é possível eliminar um objeto que esteja sob uma guarda legal.

Informações relacionadas

"Use uma conta de locatário"

"Use S3"

"Comparação do S3 Object Lock com a conformidade legada"

"Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

"Rever registos de auditoria"

Habilitando o bloqueio de objetos S3 globalmente

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

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter revisado o fluxo de trabalho do S3 Object Lock e você deve entender as considerações.
- A regra padrão na política ILM ativa deve ser compatível.

  "Criando uma regra ILM padrão"

  "Criando uma política ILM"

Sobre esta tarefa

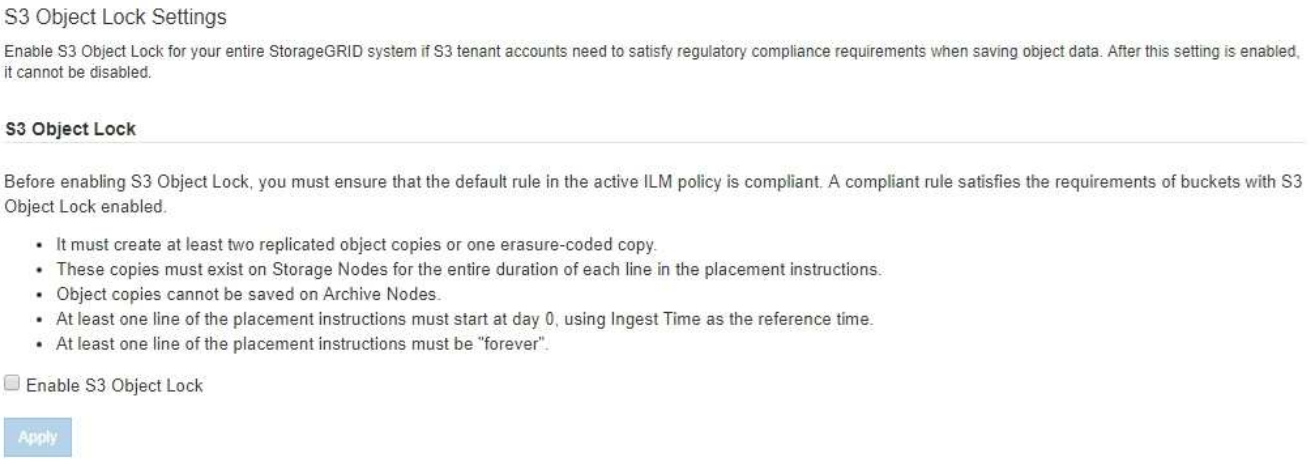
Um administrador de grade deve habilitar a configuração global S3 Object Lock para permitir que os usuários do locatário criem novos buckets com o S3 Object Lock ativado. Depois que esta definição estiver ativada, não poderá ser desativada.

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

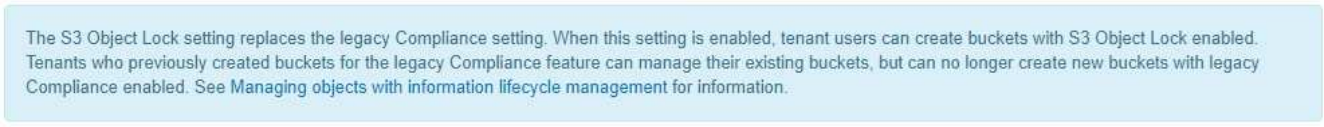
Passos

1. Selecione **Configuração** > **Definições do sistema** > **bloqueio de objetos S3**.

   A página Configurações de bloqueio de objetos S3 é exibida.

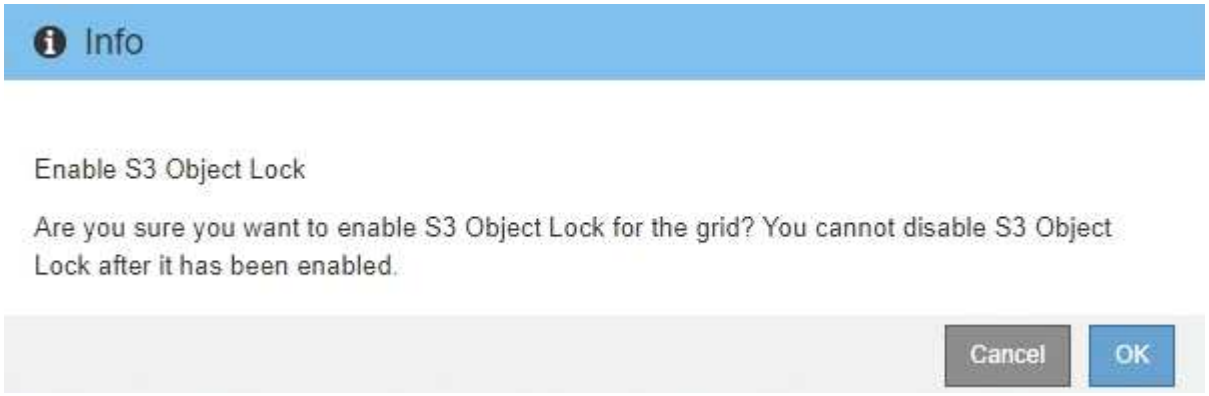


Se você ativou a configuração de conformidade global usando uma versão anterior do StorageGRID, a página inclui a seguinte nota:



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

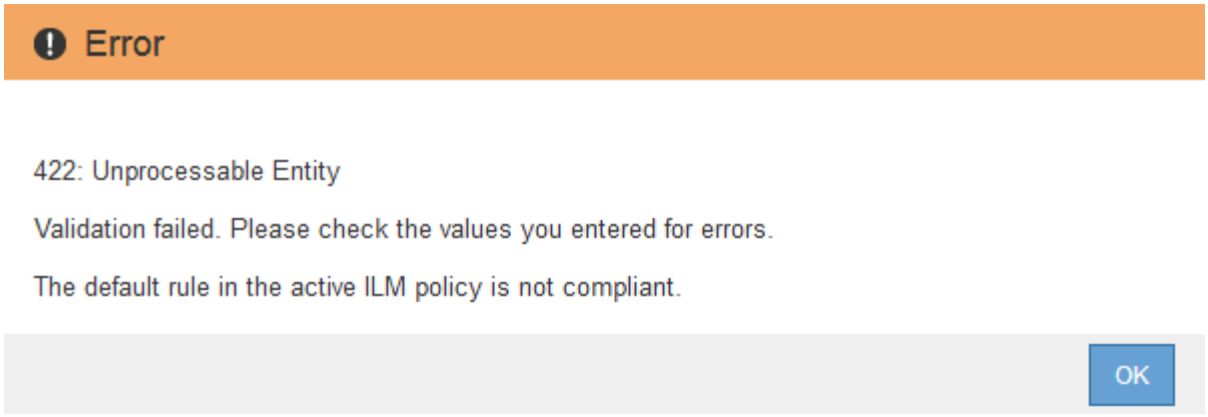
   Uma caixa de diálogo de confirmação é exibida e lembra que você não pode desativar o bloqueio de objeto S3 depois que ele estiver ativado.



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

   Quando você seleciona **OK**:

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



Depois de terminar

Depois de ativar a configuração global S3 Object Lock, você pode querer criar 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.

Informações relacionadas

"Criar uma política ILM depois que o bloqueio de objetos S3 estiver ativado"

"Criando uma regra ILM"

"Criando uma política ILM"

"Comparação do S3 Object Lock com a conformidade legada"

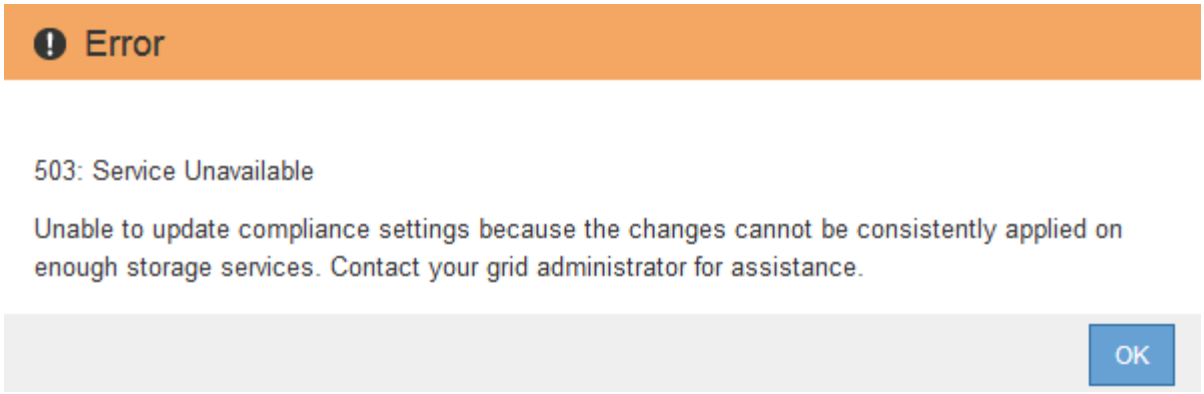
Resolução de erros de consistência ao atualizar o bloqueio de objetos S3 ou a configuração de conformidade legada

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

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

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

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



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

Para resolver esse erro, siga estas etapas:

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

Informações relacionadas

"Use uma conta de locatário"

"Use S3"

"Manter recuperar"

Exemplo de regras e políticas ILM

Você pode usar os exemplos nesta seção como um ponto de partida para suas próprias regras e políticas ILM.

- "Exemplo 1: Regras e política de ILM para armazenamento de objetos"
- "Exemplo 2: Regras de ILM e política para filtragem de tamanho de objeto EC"
- "Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem"
- "Exemplo 4: Regras ILM e política para objetos com versão S3"
- "Exemplo 5: Regras de ILM e política para comportamento de ingestão rigorosa"
- "Exemplo 6: Alterando uma política ILM"
- "Exemplo 7: Política de ILM compatível para bloqueio de objetos S3"

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

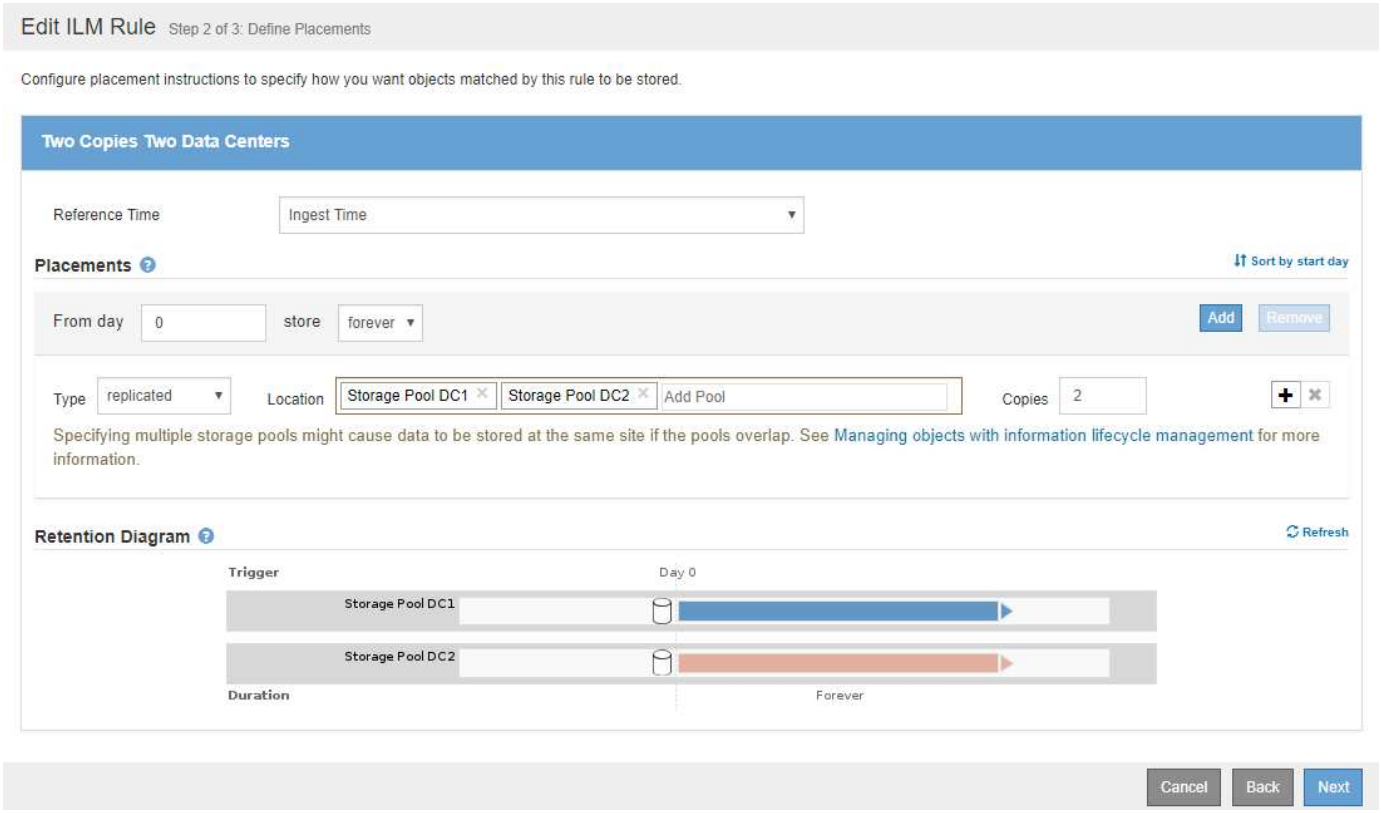
objetos.

> 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 objetos para dois data centers

Este exemplo de regra de ILM copia dados de objetos para pools de storage em dois data centers.

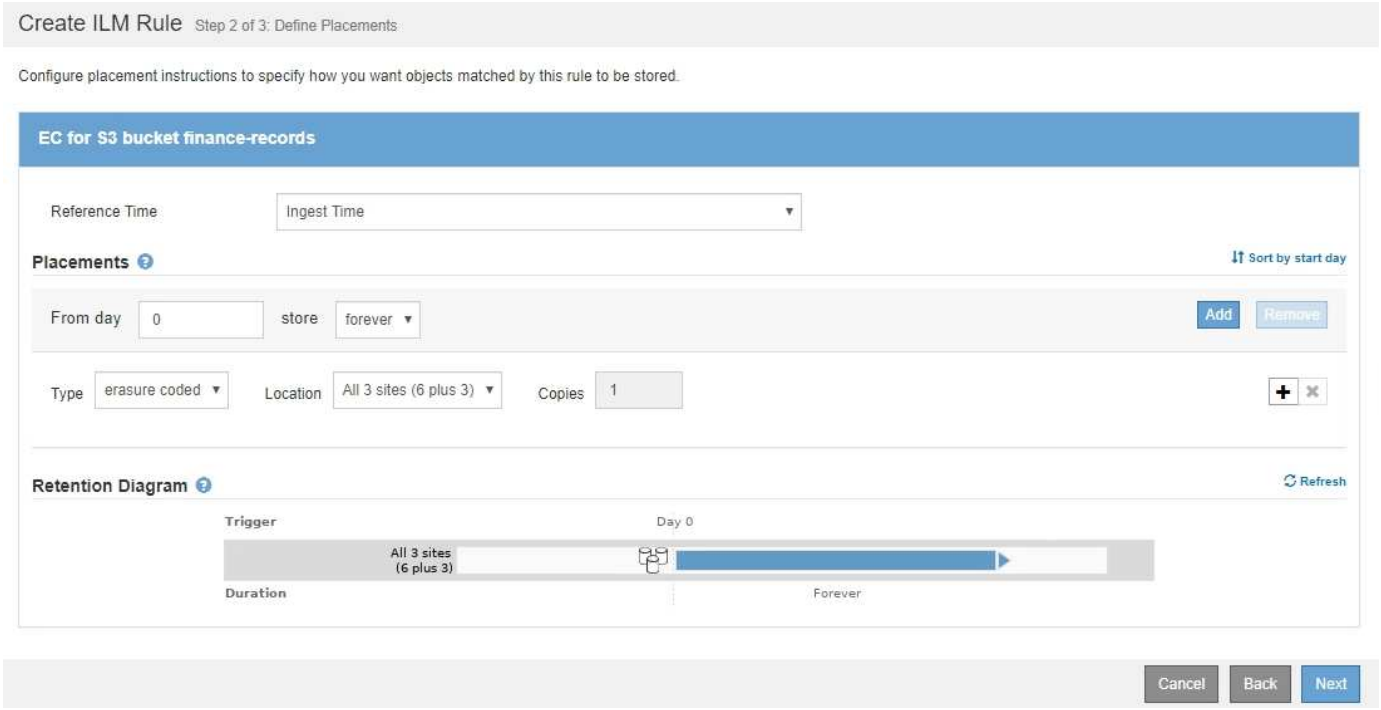
Definição de regra	Exemplo de valor
Pools de armazenamento	Dois pools de storage, cada um em data centers diferentes, denominados Storage Pool DC1 e Storage Pool DC2.
Nome da regra	Duas cópias de dois data centers
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre: Uma no Storage Pool DC1 e uma no Storage Pool DC2.



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
Perfil de codificação de apagamento	• Um pool de storage em três data centers (todos os 3 locais) • Use o esquema de codificação de apagamento 6-3
Nome da regra	EC para Registros financeiros do bucket S3
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	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.



Política de ILM, por exemplo, 1

O sistema StorageGRID permite que você projete políticas sofisticadas e complexas de ILM; no entanto, na prática, a maioria das políticas de ILM são simples.

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

- Na ingestão, use a codificação de apagamento 6-3 para armazenar todos os objetos pertencentes ao bucket S3 nomeados `finance-records` em três data centers.
- 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 em dois data centers, DC1 e DC2.

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

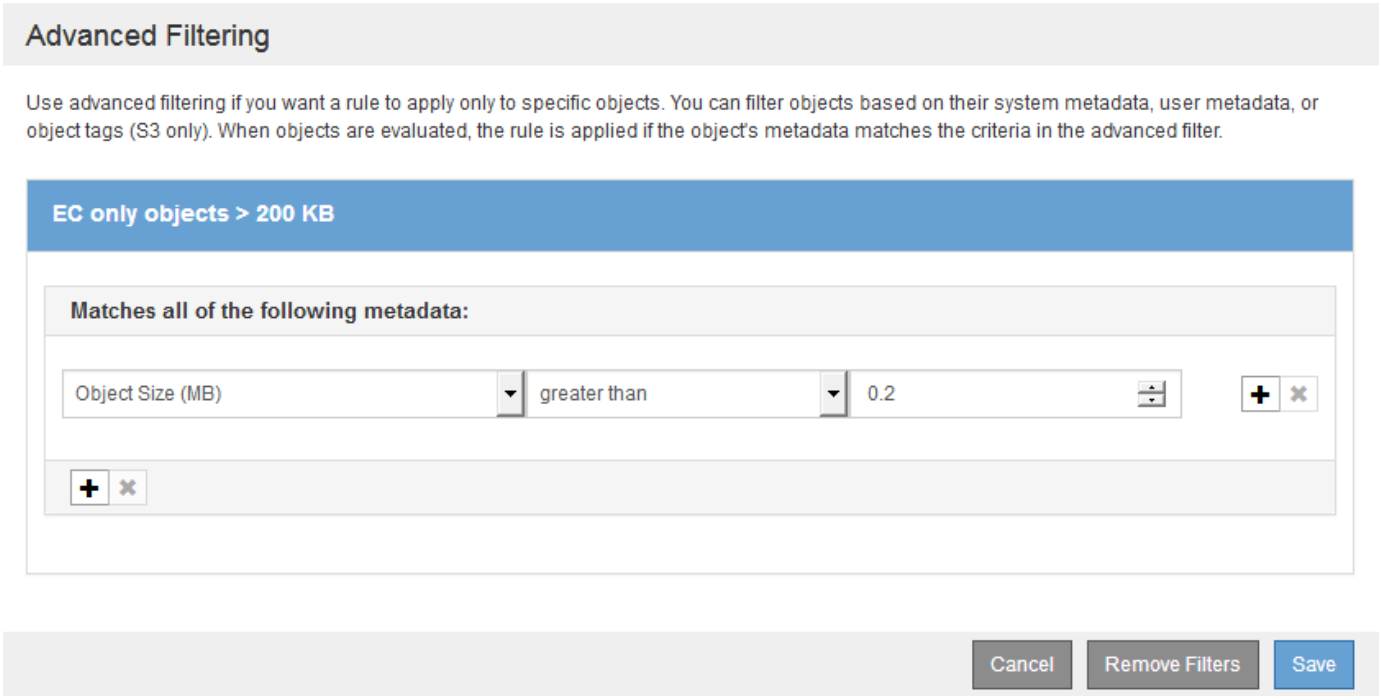
definir uma política de ILM que filtra por tamanho do objeto para atender aos requisitos de EC recomendados.

> 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.

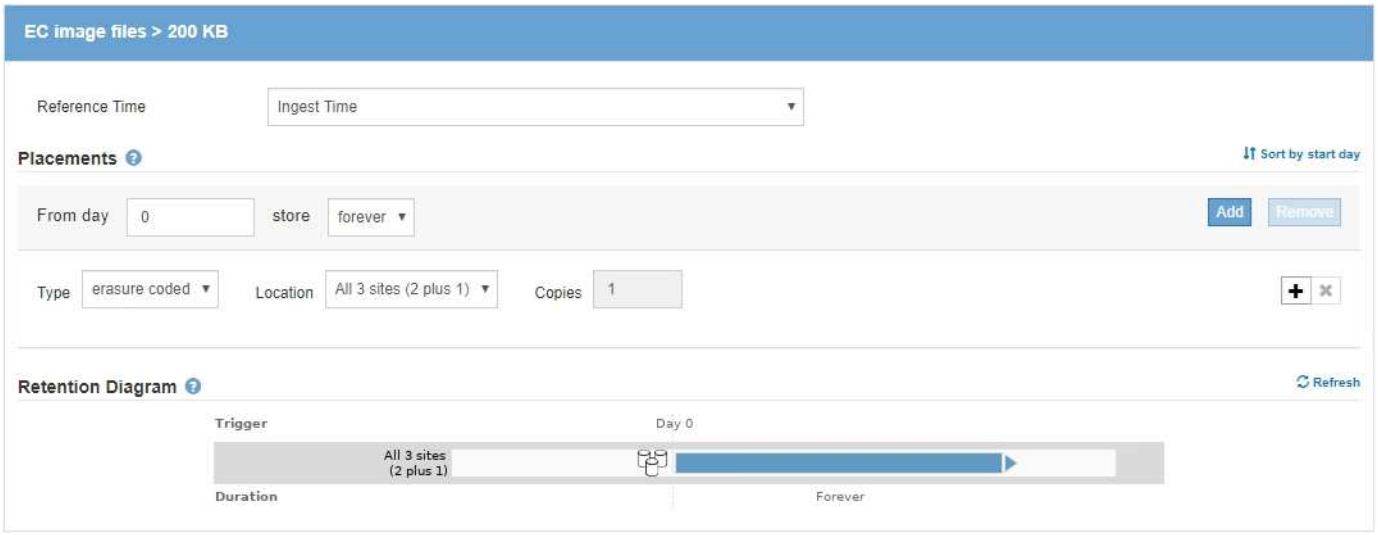
Regra ILM 1 por exemplo 2: Use EC para todos os objetos maiores que 200 KB

Este exemplo de exclusão de regra ILM codifica todos os objetos com mais de 200 KB (0,20 MB).

Definição de regra	Exemplo de valor
Nome da regra	Objetos somente EC > 200 KB
Tempo de referência	Tempo de ingestão
Filtragem Avançada para tamanho Objeto	Tamanho do objeto (MB) maior que 0,20
Colocação de conteúdo	Crie uma cópia codificada por apagamento 2-1 usando três sites



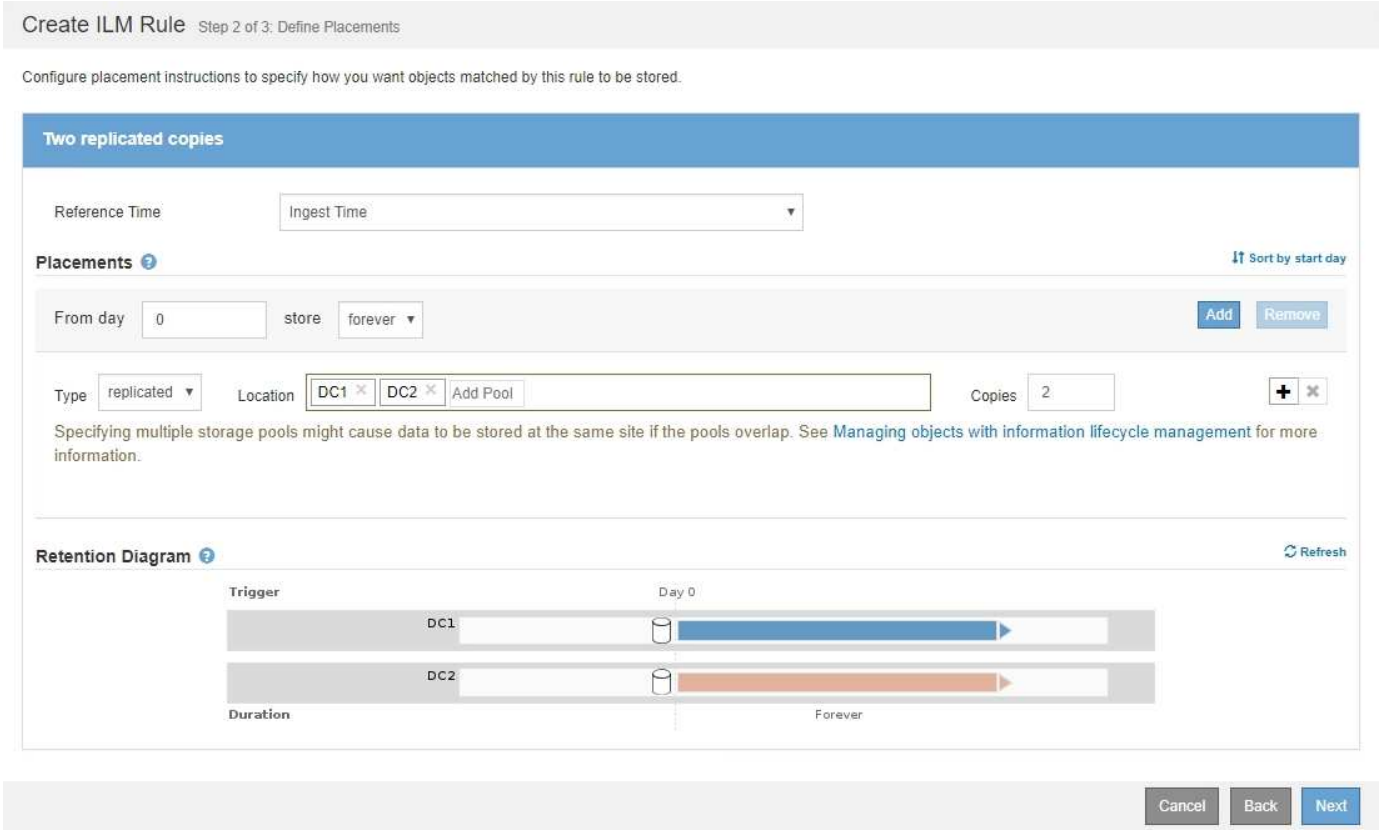
As instruções de colocação especificam que uma cópia codificada por apagamento 2-1 seja criada usando todos os três sites.



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 segunda regra da política. Como a regra ILM 1, por exemplo, 2, filtra todos os objetos maiores que 200 KB, a regra ILM 2, por exemplo, 2, aplica-se apenas a objetos com 200 KB ou menores.

Definição de regra	Exemplo de valor
Nome da regra	Duas cópias replicadas
Tempo de referência	Tempo de ingestão
Filtragem Avançada para tamanho Objeto	Nenhum
Colocação de conteúdo	Crie duas cópias replicadas e salve-as em dois data centers, DC1 e DC2



Política de ILM, por exemplo, 2: Use EC para objetos maiores que 200 KB

Nesta política de exemplo, objetos com mais de 200 KB são codificados para apagamento. Duas cópias replicadas são feitas de todos os outros objetos.

Este exemplo de política ILM inclui as seguintes regras ILM:

- Codificar para apagamento todos os objetos com mais de 200 KB.
- Se um objeto não corresponder à primeira regra ILM, use a regra ILM padrão para criar duas cópias replicadas desse objeto. Como objetos com mais de 200 KB foram filtrados pela regra 1, a regra 2 aplica-se apenas a objetos com 200 KB ou menos.

Exemplo 3: Regras e política de ILM para melhor proteção para arquivos de imagem

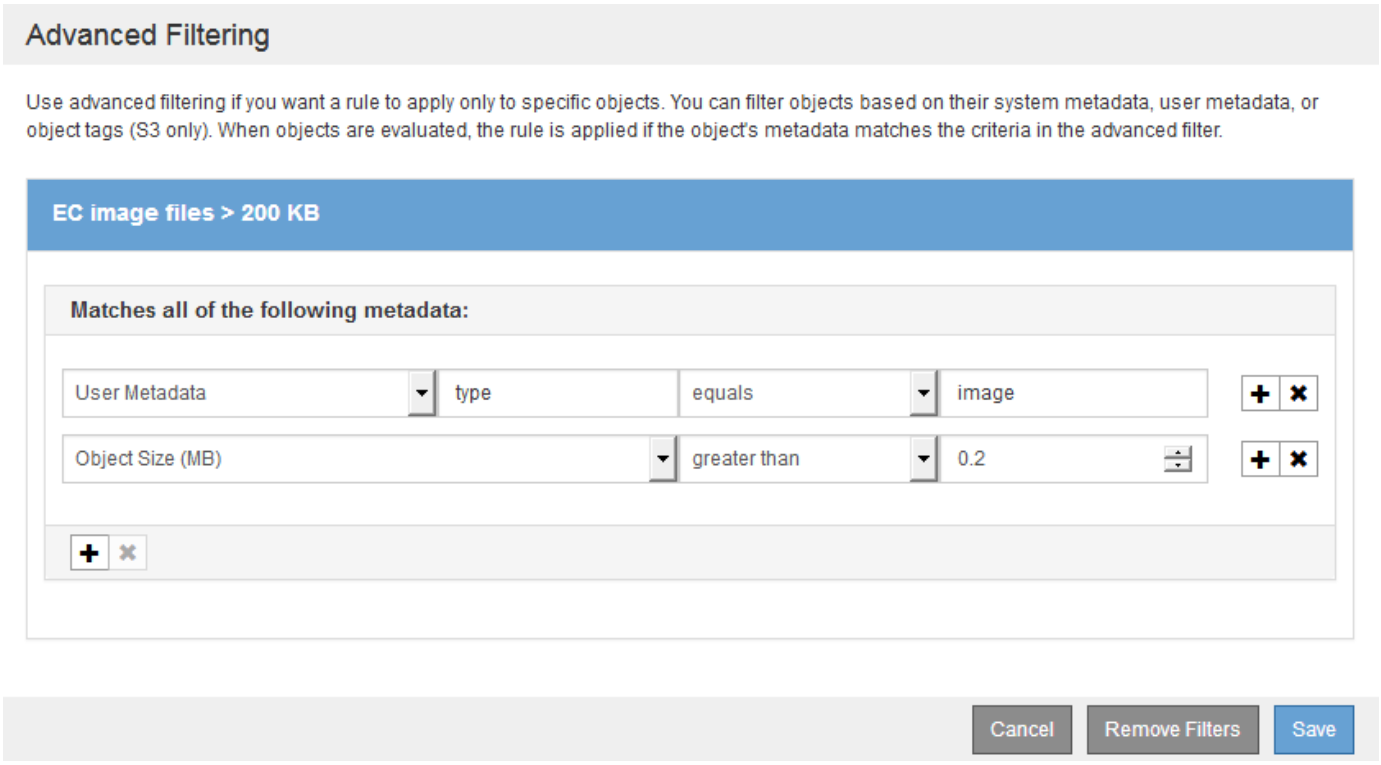
Você pode usar as regras e a política de exemplo a seguir para garantir que imagens maiores de 200 KB sejam codificadas para apagamento e que três cópias sejam feitas de imagens menores.

> 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.

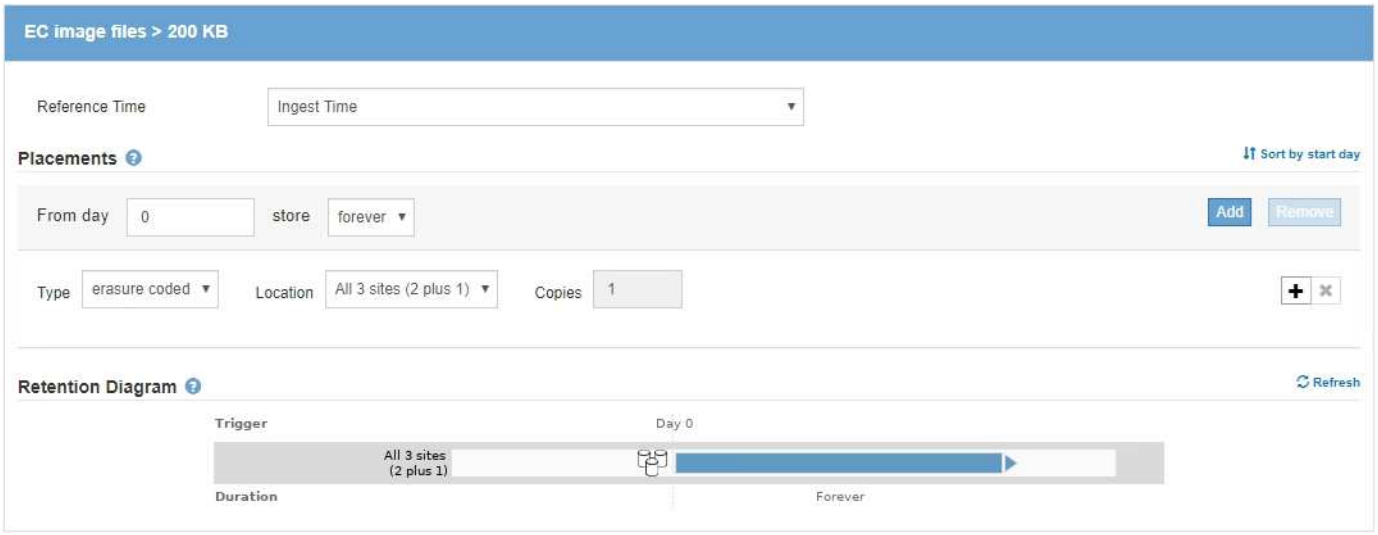
Regra ILM 1 por exemplo 3: Use EC para arquivos de imagem maiores que 200 KB

Este exemplo de regra ILM usa filtragem avançada para codificar todos os arquivos de imagem com mais de 200 KB.

Definição de regra	Exemplo de valor
Nome da regra	Ficheiros de imagem EC > 200 KB
Tempo de referência	Tempo de ingestão
Filtragem avançada para metadados do usuário	O tipo de metadados do usuário é igual a arquivos de imagem
Filtragem Avançada para tamanho Objeto	Tamanho do objeto (MB) maior que 0,2
Colocação de conteúdo	Crie uma cópia codificada por apagamento 2-1 usando três sites



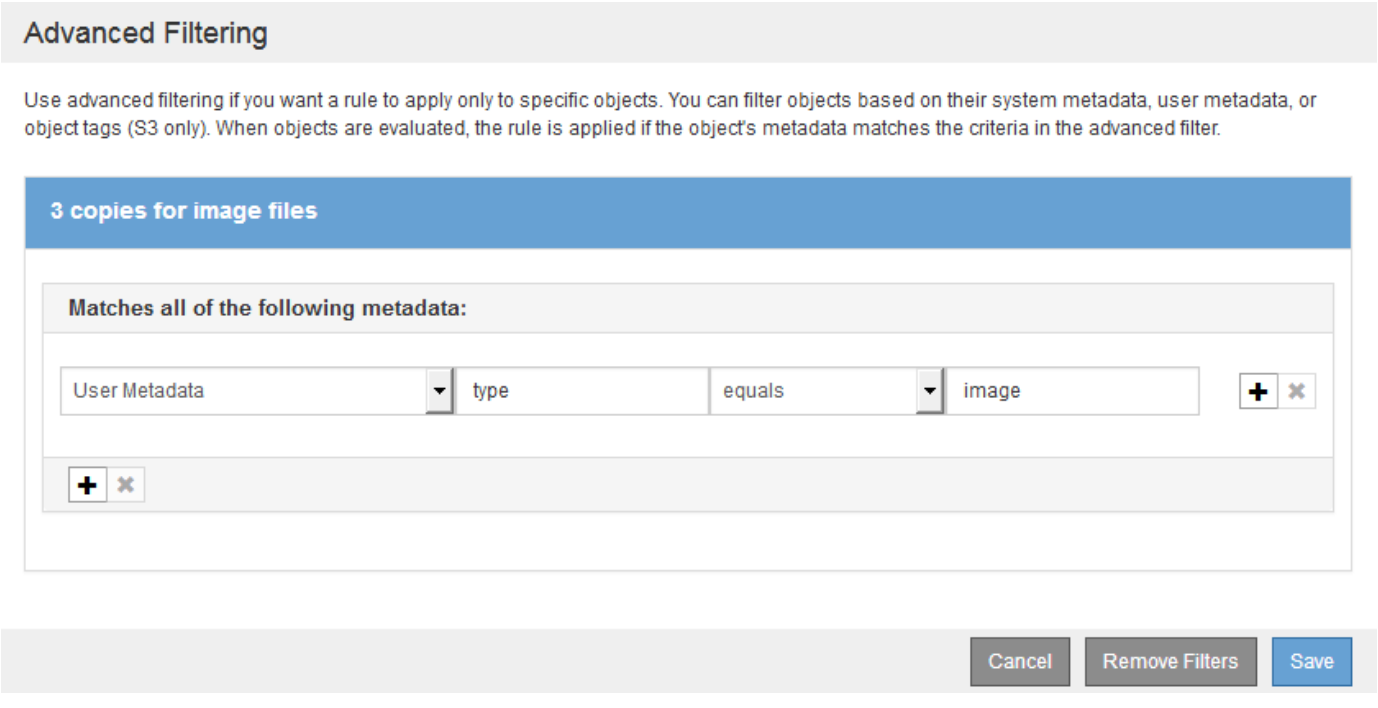
Como essa regra é configurada como a primeira regra na política, a instrução de posicionamento de codificação de apagamento só se aplica a imagens maiores que 200 KB.



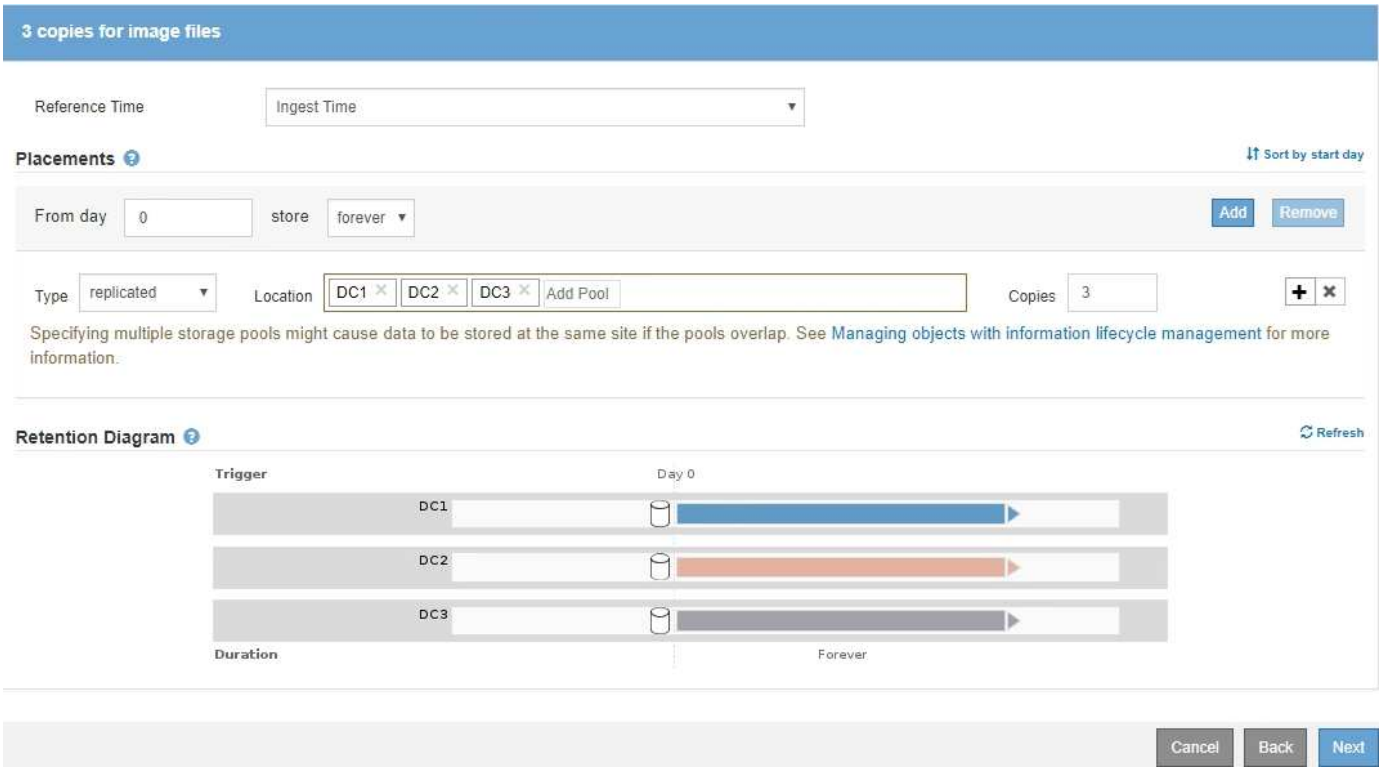
Regra ILM 2 por exemplo 3: Replique 3 cópias para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que os arquivos de imagem sejam replicados.

Definição de regra	Exemplo de valor
Nome da regra	3 cópias para arquivos de imagem
Tempo de referência	Tempo de ingestão
Filtragem avançada para metadados do usuário	O tipo de metadados do usuário é igual a arquivos de imagem
Colocação de conteúdo	Crie 3 cópias replicadas em todos os nós de storage



Como a primeira regra na política já corresponde a arquivos de imagem maiores que 200 KB, essas instruções de colocação só se aplicam a arquivos de imagem 200 KB ou menores.



Política ILM, por exemplo, 3: Melhor proteção para arquivos de imagem

Neste exemplo, a política ILM usa três regras ILM para criar uma política que codifique arquivos de imagem com mais de 200 KB (0,2 MB), crie cópias replicadas para arquivos de imagem com 200 KB ou menos e faça duas cópias replicadas para qualquer arquivo que não seja de imagem.

Este exemplo de política ILM inclui regras que executam o seguinte:

- Todos os arquivos de imagem com mais de 200 KB.
- Crie três cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 200 KB ou menos).
- Aplique a regra padrão a quaisquer objetos restantes (ou seja, todos os 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 na política do ILM que usam **hora não atual** como tempo de referência.

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.

Se você criar políticas ILM para gerenciar versões de objetos não atuais, saiba que você deve conhecer o UUID ou CBID da versão do objeto para simular a política. Para encontrar UUUID e CBID de um objeto, use Object Metadata Lookup enquanto o objeto ainda estiver atual.

Informações relacionadas

"Como objetos com versão S3 são excluídos"

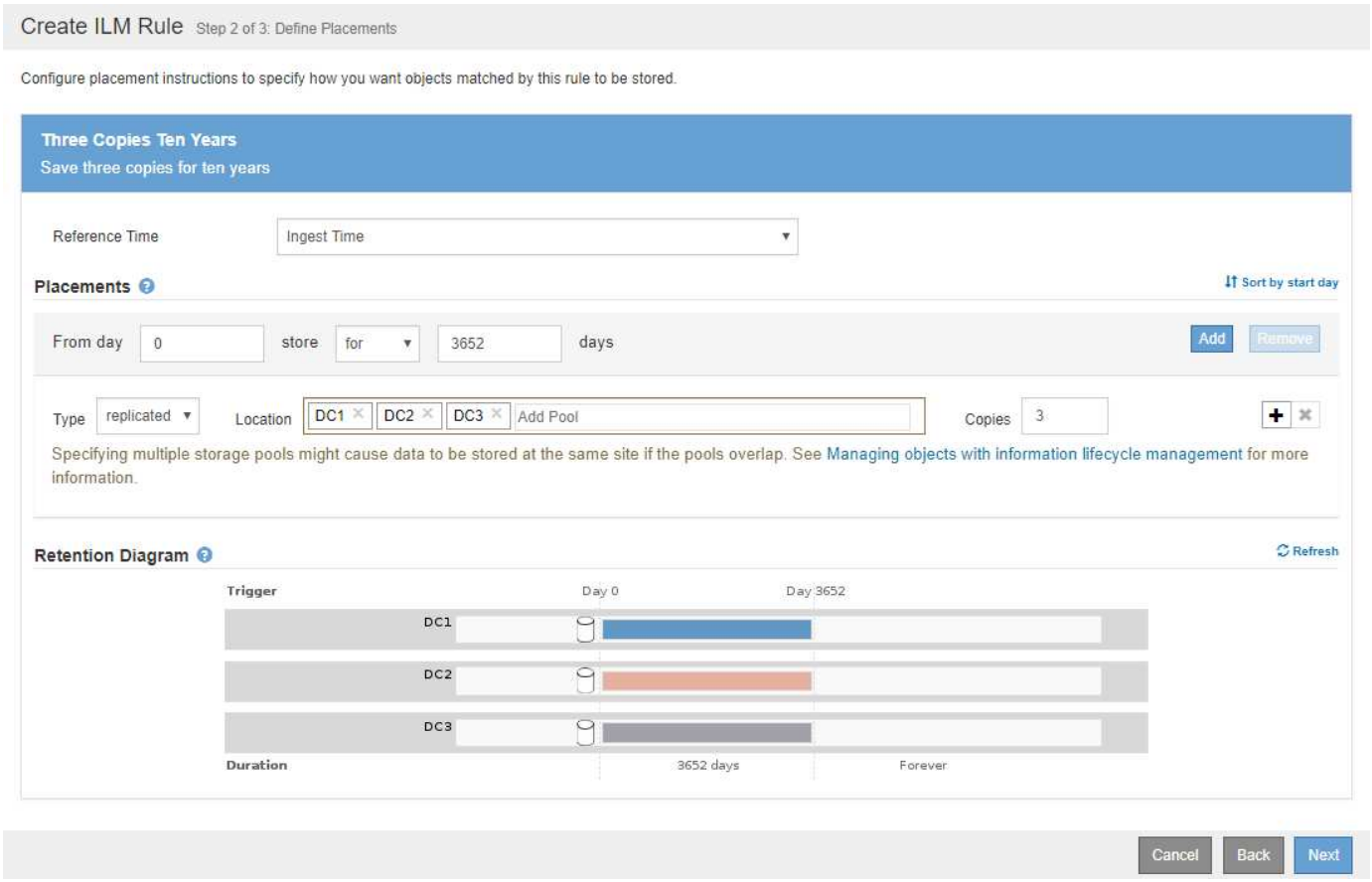
"Verificando uma política ILM com pesquisa de metadados de objeto"

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 data centers 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 storage, cada um em data centers diferentes, denominados DC1, DC2 e DC3.
Nome da regra	Três cópias dez anos
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma em DC1, uma em DC2 e uma em DC3. No final de 10 anos, exclua todas as cópias do objeto.



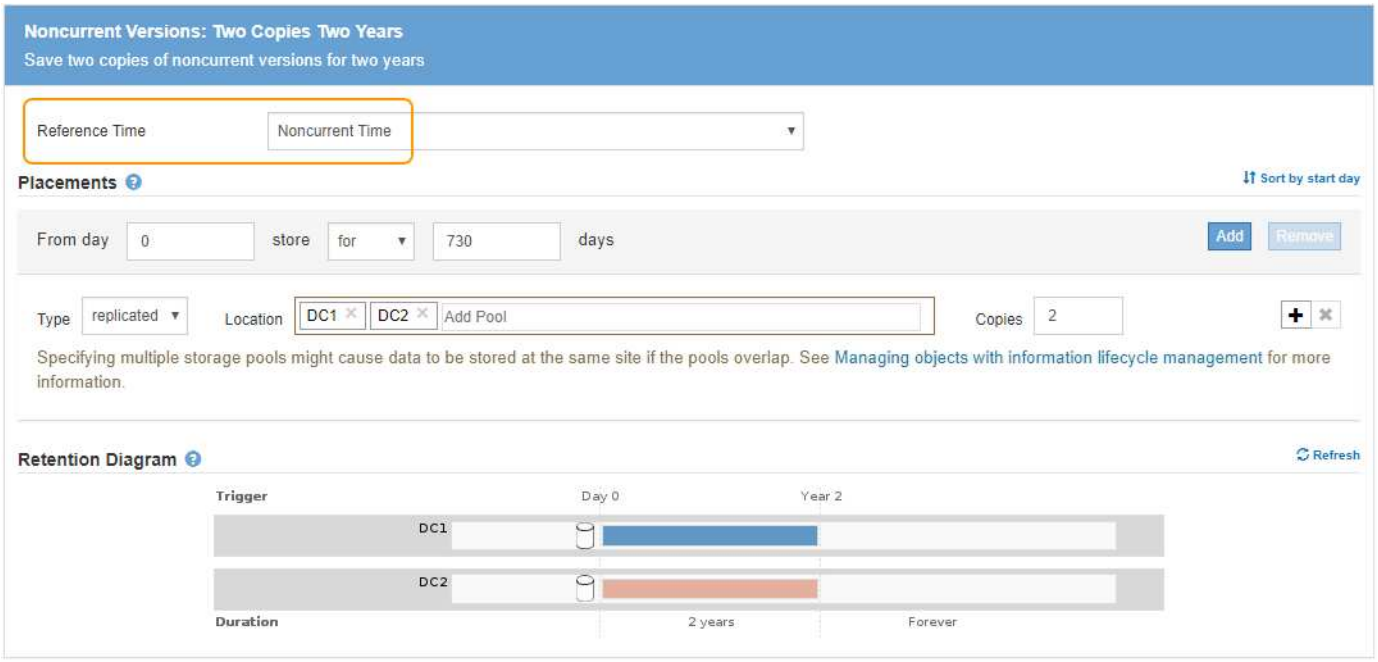
Regra ILM 2 por exemplo 4: Salve duas cópias de versões não atuais por 2 anos

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. Esta regra usa a opção **hora não atual** para hora de referência.

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 storage, cada um em data centers diferentes, denominados DC1 e DC2.
Nome da regra	Versões não atuais: Duas cópias dois anos
Tempo de referência	Hora não atual
Colocação de conteúdo	No dia 0 em relação à hora 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 em DC1 e uma em DC2. 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 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 tempo 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 de tempo não atual.

- Na obtenção, crie três cópias replicadas e armazene uma cópia em cada um dos três data centers. 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 estiver atual, você pode usar a Pesquisa de metadados de Objeto para encontrar seus UUID e CBID.

- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto for 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 ILM ocorrer, essa versão não atual é correspondida pela primeira regra. Como resultado, a cópia em DC3 é purgada e as duas cópias em DC1 e DC2 são armazenadas por mais 2 anos.

Informações relacionadas

"Verificando uma política ILM com pesquisa de metadados de objeto"

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

"Como os objetos são ingeridos"

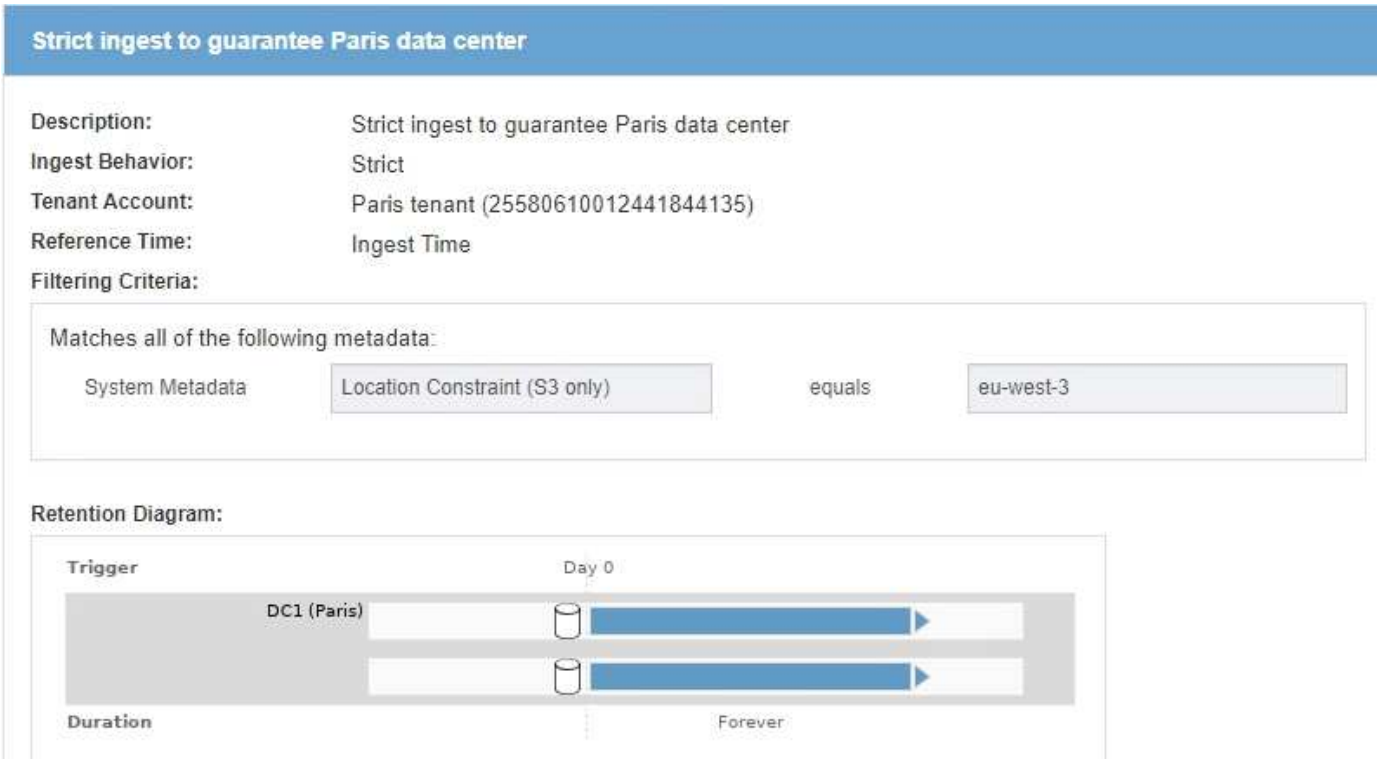
"Etapa 3 de 3: Definir o comportamento de ingestão"

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
Filtragem avançada	A restrição de localização é igual à eu-West-3
Pools de armazenamento	DC1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre em DC1 (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.



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.

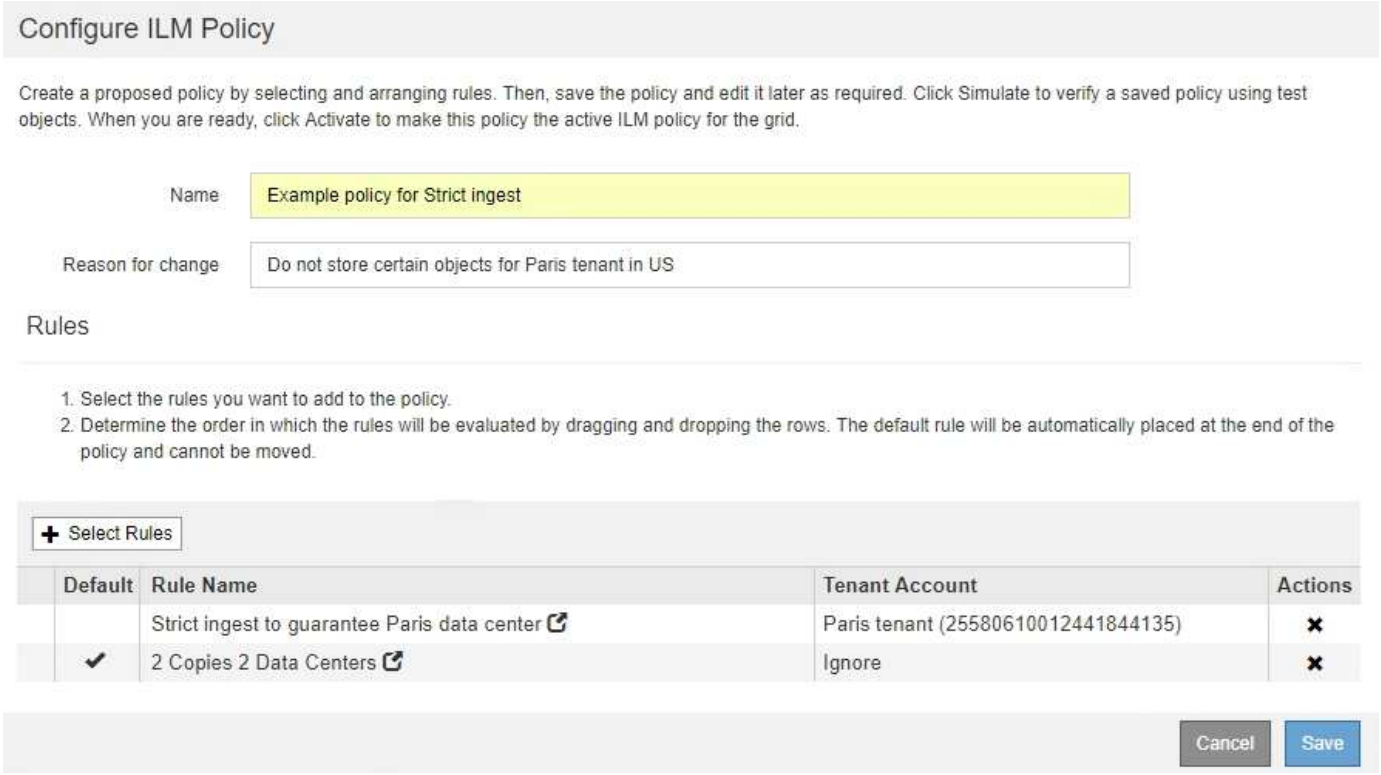
Definição de regra	Exemplo de valor
Conta de locatário	Ignorar
Filtragem avançada	*Não especificado*
Pools de armazenamento	DC1 (Paris) e DC2 (EUA)
Nome da regra	2 cópias 2 Data Centers
Tempo de referência	Tempo de ingestão
Colocação de conteúdo	No dia 0, mantenha duas cópias replicadas para sempre em 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: Alterando uma política ILM

Talvez seja necessário criar e ativar uma nova política de ILM se sua proteção de dados precisar mudar ou adicionar novos sites.

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 a política ILM ativa precisa ser revisada para armazenar dados no novo site.

> 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 a alteração de 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.

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.

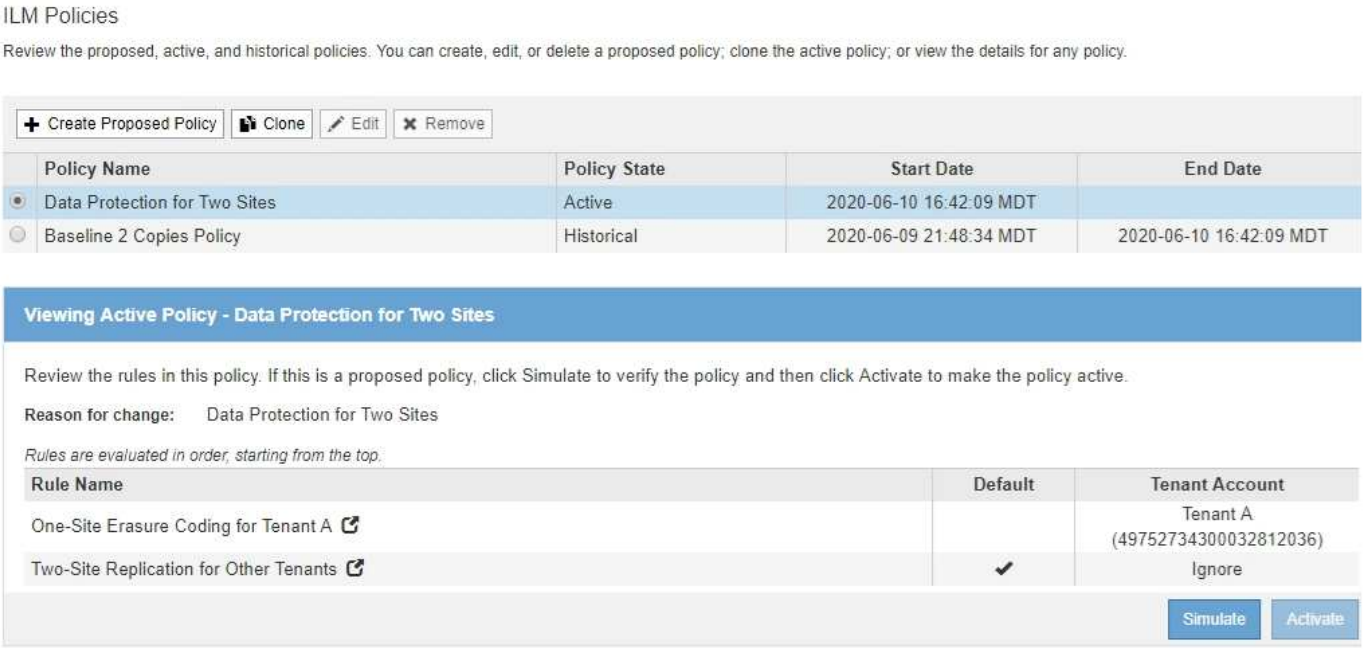
- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos codificados por apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos de ou para um pool de armazenamento em nuvem ou de ou para um local remoto.

Informações relacionadas

"Criando uma política ILM"

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.



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 de 200 KB será protegido pela segunda regra, 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	Centro de dados 1
Colocação de conteúdo	Codificação de apagamento 2-1 no Data Center 1 do dia 0 para sempre

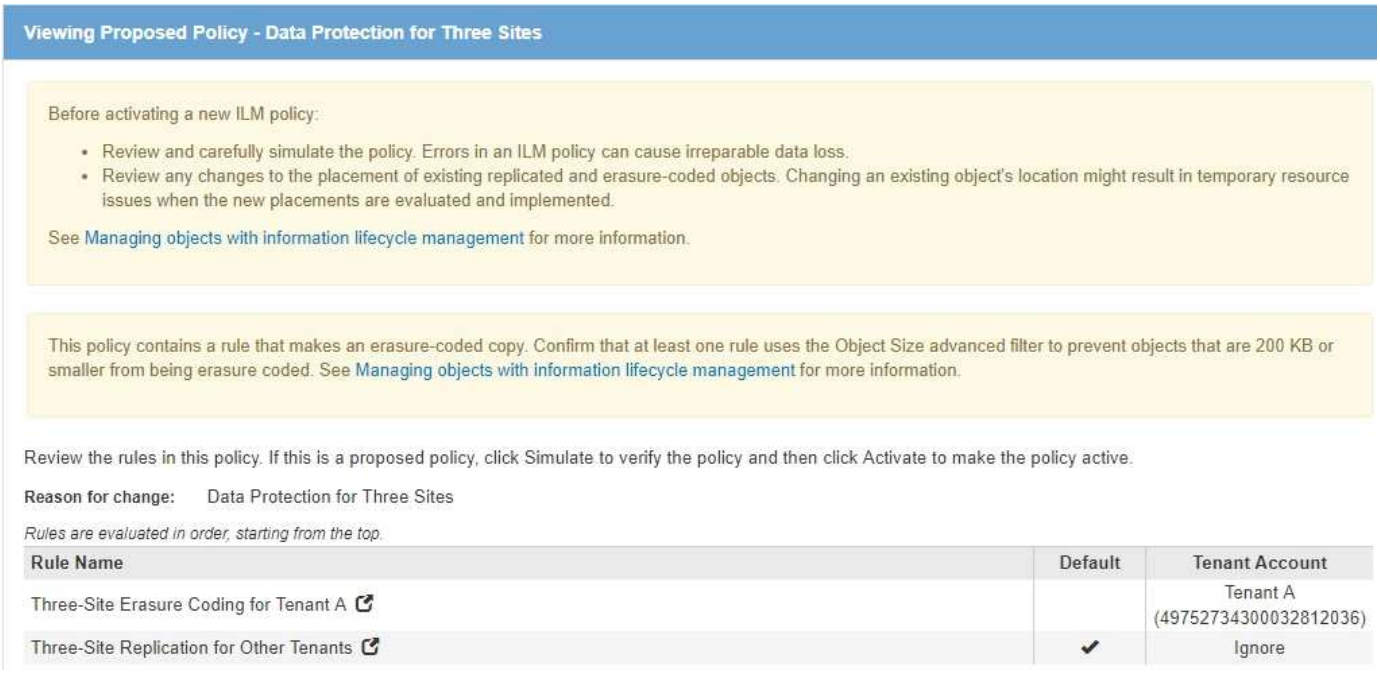
Regra 2: Replicação de dois locais para outros locatários

Definição de regra	Exemplo de valor
Nome da regra	Replicação de dois locais para outros locatários
Conta de locatário	Ignorar
Pools de armazenamento	Data Center 1 e data center 2
Colocação de conteúdo	Duas cópias replicadas do dia 0 para sempre: Uma cópia no data center 1 e uma cópia no data center 2.

Proposta de política de ILM, por exemplo, 6: Proteção de dados em três locais

Neste exemplo, a política ILM está sendo atualizada para um sistema StorageGRID de três locais.

Depois de executar uma expansão para adicionar o novo local, o administrador de grade criou dois novos pools de storage: Um pool de storage para o Data Center 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 3 Data Centers (inclui Data Center 1, Data Center 2 e Data Center 3)
Colocação de conteúdo	Codificação de apagamento 2-1 em todos os 3 Data Centers, desde o dia 0 até 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	Data Center 1, Data Center 2 e Data Center 3
Colocação de conteúdo	Três cópias replicadas do dia 0 para sempre: Uma cópia no data center 1, uma cópia no data center 2 e uma cópia no data center 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 Data Center 1. Na nova política proposta de ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2-1 nos Data Centers 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 data center 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 data centers.

> Os fragmentos 2 mais 1 existentes no Data Center 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 Data Centers 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 Data Centers 1, 2 e 3.

Quando a nova política ILM é ativada, ocorrem as seguintes operações ILM:

- Quando qualquer Locatário que não o Locatário A ingere um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada data center.
- 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 Data Center 1 e no Data Center 2 continuam atendendo aos requisitos de replicação da nova regra ILM, o StorageGRID só precisa criar uma nova cópia do objeto para o Data Center 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 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 Data Center 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 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

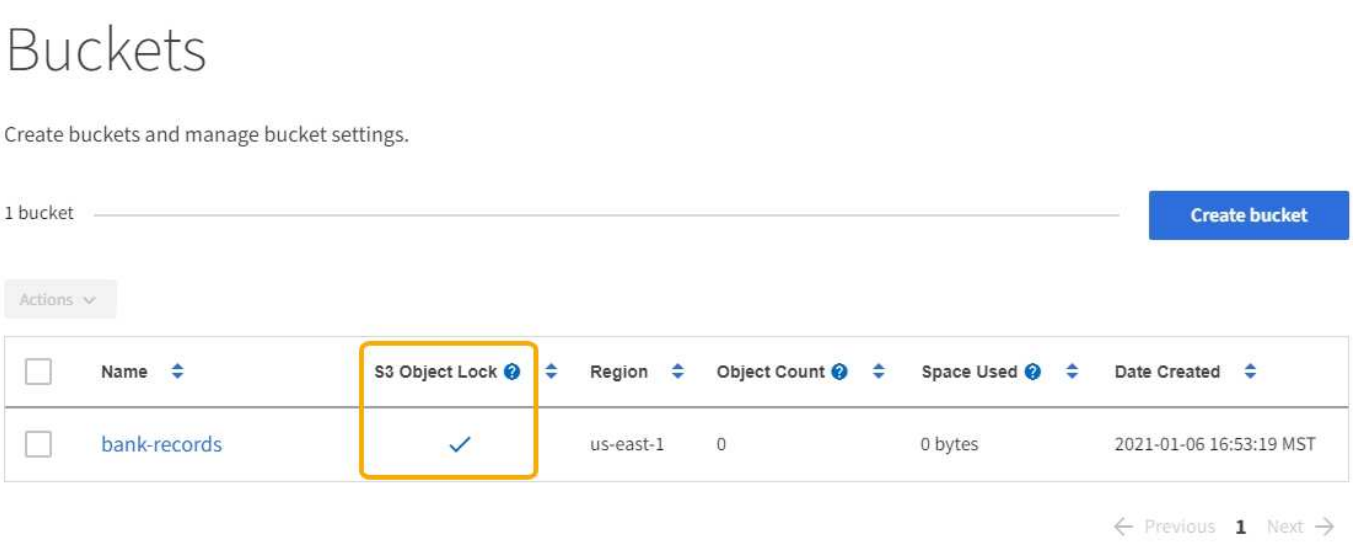
"Gerenciando objetos com o S3 Object Lock"

"Criando 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	registos 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`.

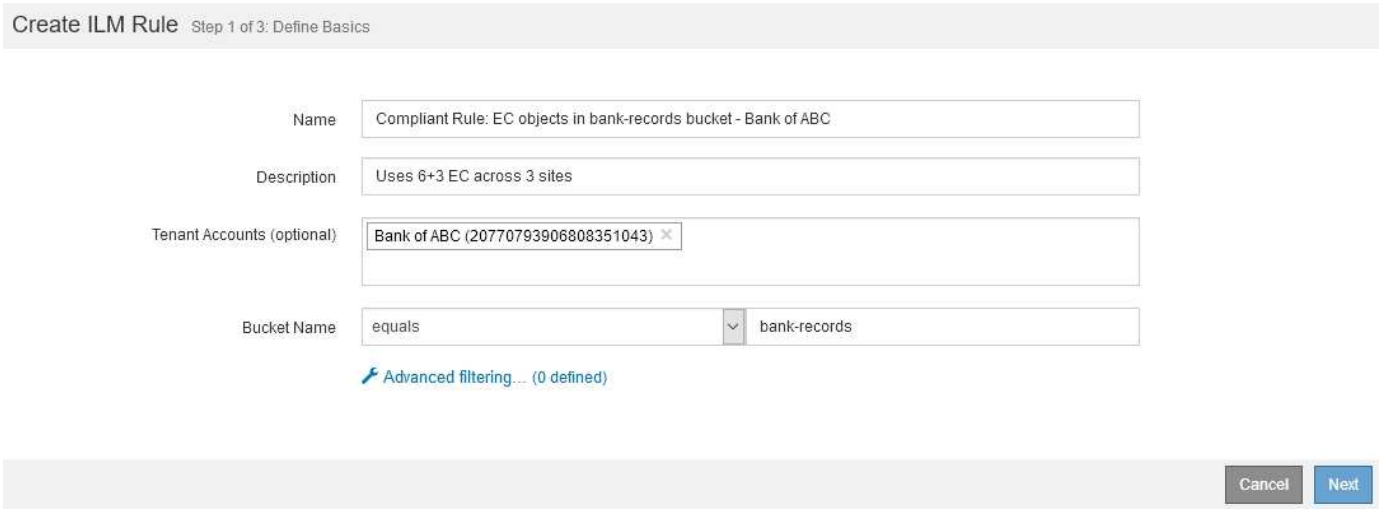
Definição para cada objeto	Exemplo de valor
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 de dezembro de 2030) Cada versão de objeto tem sua `retain-until-date` própria configuração. Esta definição pode ser aumentada, mas não diminuída.
`legal hold`	`"OFF"` (Não em vigor) Uma retenção legal pode ser 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 pode ser excluído mesmo que o `retain-until-date` tenha sido alcançado.

Regra 1 do ILM para o bloqueio de objetos S3 exemplo: Perfil de codificação de apagamento com correspondência de bucket

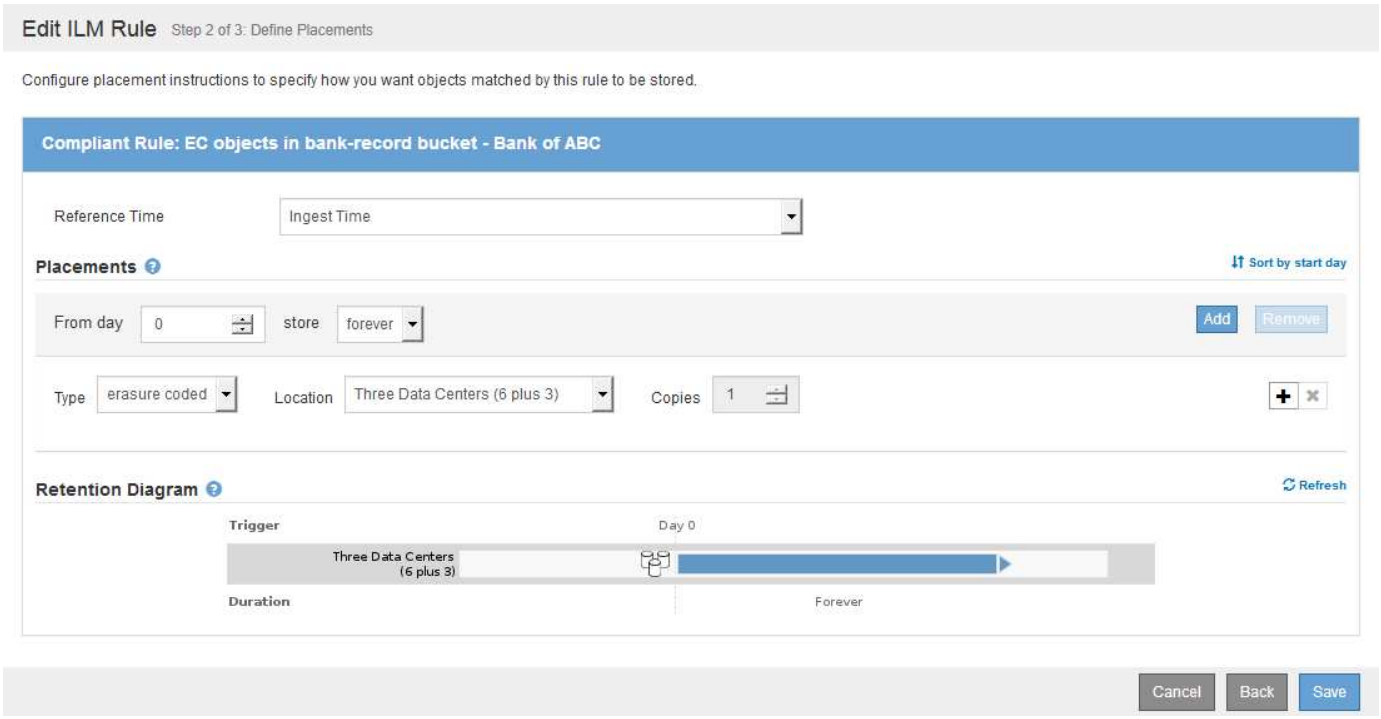
Este exemplo de regra ILM aplica-se apenas à conta de locatário S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa a codificação de apagamento para armazenar o objeto em nós de storage em três locais de data center usando um 6 perfil de codificação de apagamento de mais de 3 anos. Essa regra atende aos requisitos dos buckets com o S3 Object Lock ativado: Uma cópia codificada por apagamento 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 - Bank of ABC
Conta de locatário	Banco do ABC

Definição de regra	Exemplo de valor
Nome do balde	`bank-records`
Filtragem avançada	Tamanho do objeto (MB) maior que 0,20 **Nota:** este filtro garante que a codificação de apagamento não seja usada para objetos de 200 KB ou menores.



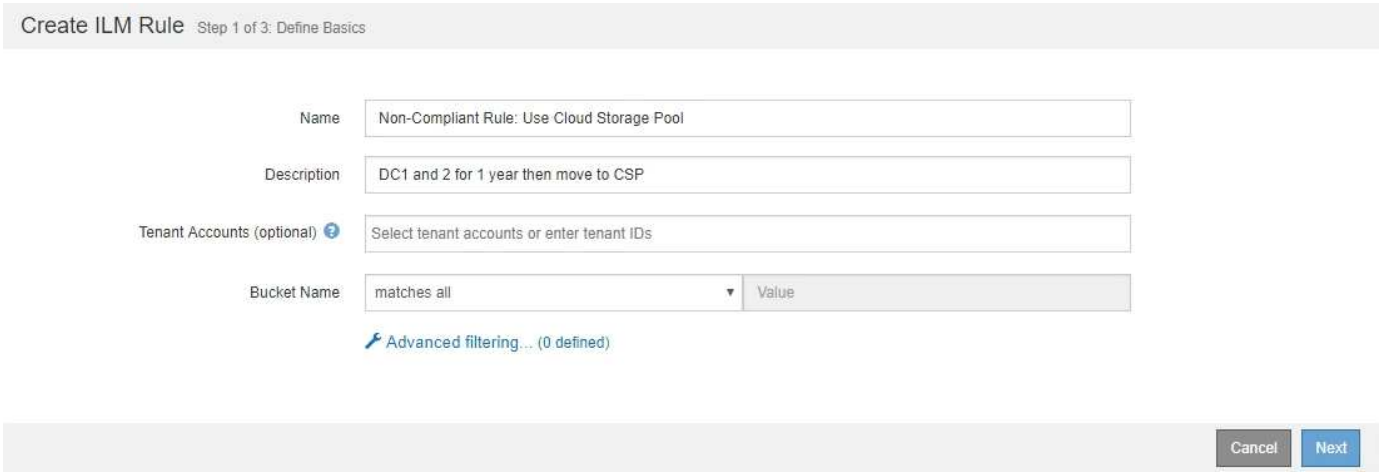
Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	Desde o dia 0 loja para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada por apagamento em nós de storage em três locais de data center • Usa o esquema de codificação de apagamento 6-3



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 balde	Não especificado, mas só se aplicará a buckets que não tenham o bloqueio de objeto S3 (ou o recurso de conformidade legado) habilitado.
Filtragem avançada	Não especificado

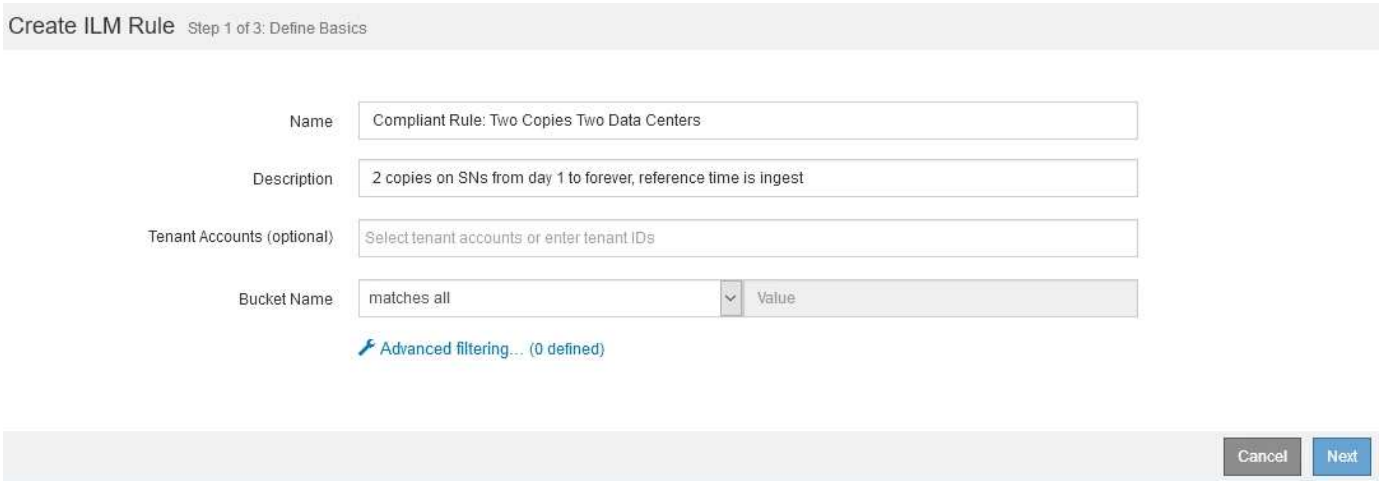


Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
Colocações	• No dia 0, mantenha duas cópias replicadas nos nós de storage no data center 1 e no data center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um pool de storage de nuvem para sempre

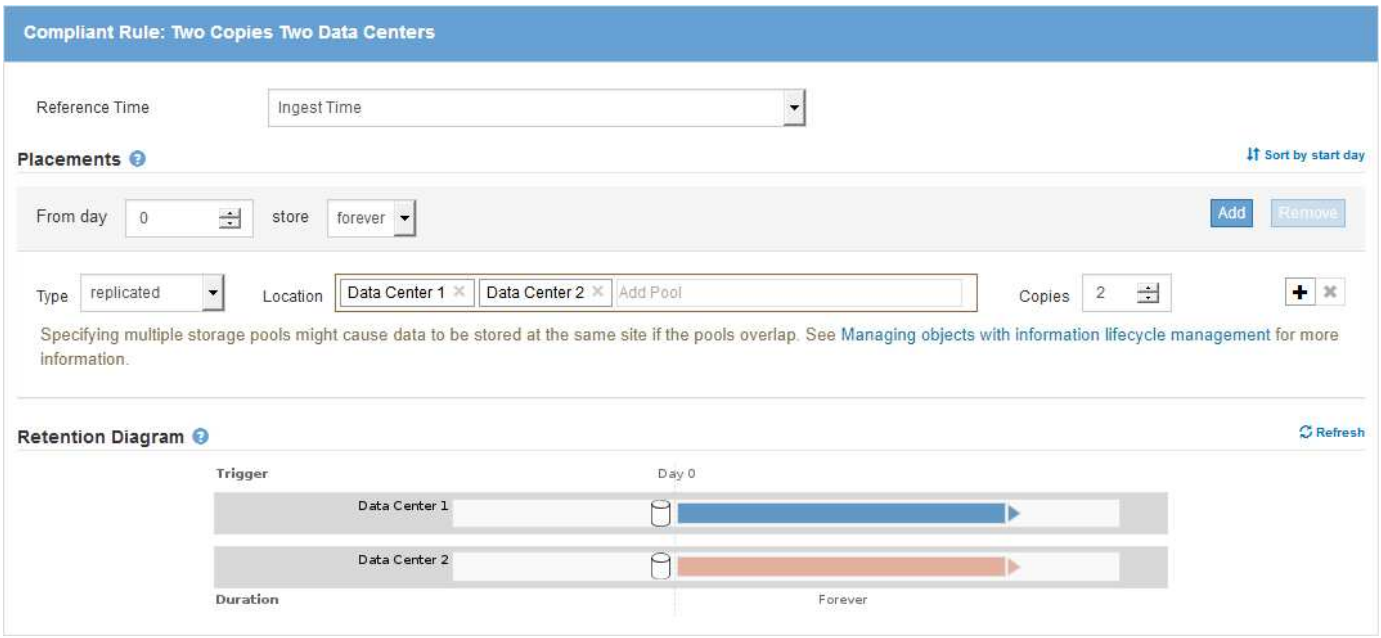
Regra ILM 3 para o exemplo de bloqueio de objetos S3: Regra padrão

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 e atende aos requisitos dos buckets com o bloqueio de objeto S3 ativado: Duas cópias de objeto são mantidas nos nós de storage 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 balde	Não especificado
Filtragem avançada	Não especificado



Definição de regra	Exemplo de valor
Tempo de referência	Tempo de ingestão
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.

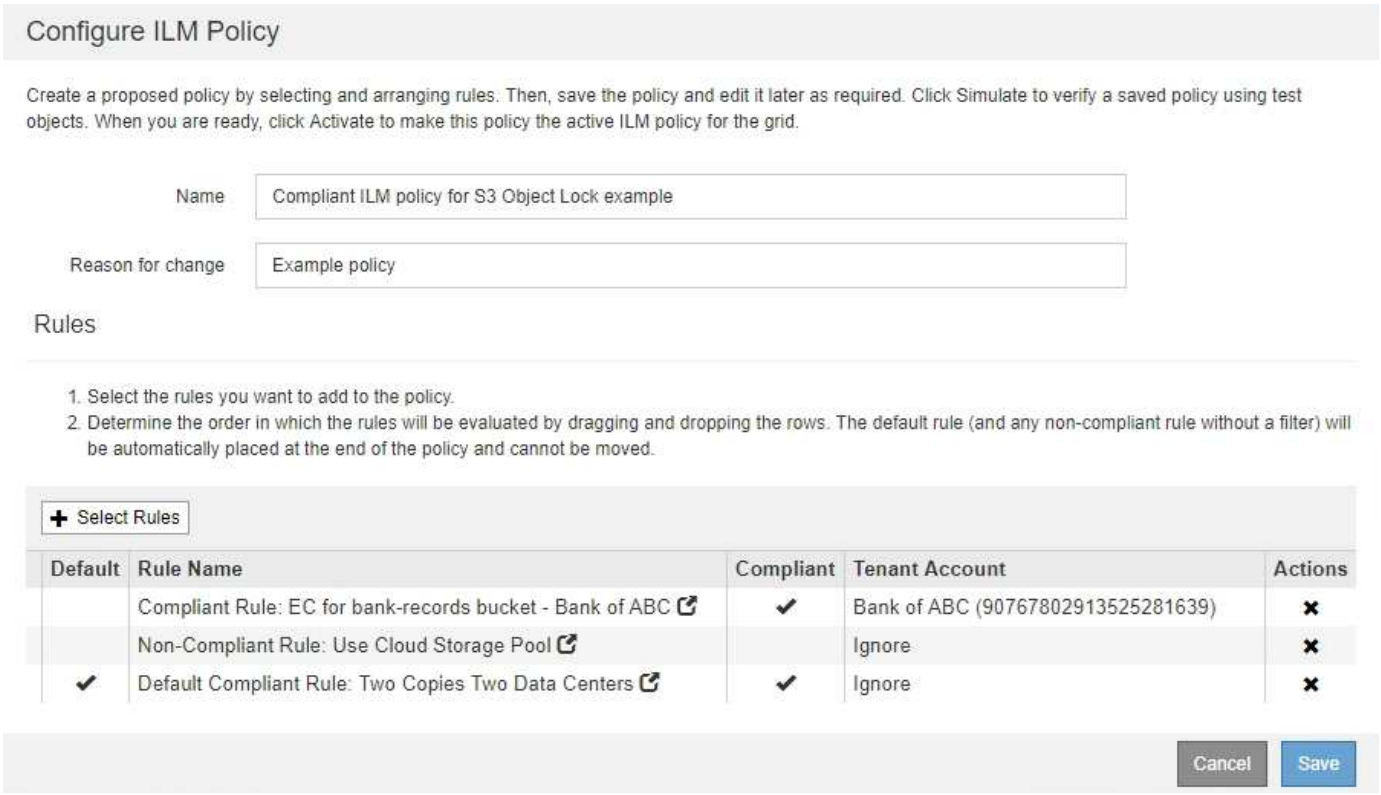
Adicionando regras à política

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 200 KB 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.



Simulando 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 200 KB 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 200 KB 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.

Ativar 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

Informações sobre marcas comerciais