Gerenciar objetos com ILM

StorageGRID software

NetApp
December 03, 2025

Índice

Gerenciar objetos com ILM

Gerenciar objetos com ILM

As regras de gerenciamento do ciclo de vida das informações (ILM) em uma política de ILM instruem o StorageGRID sobre como criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Sobre estas instruções

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

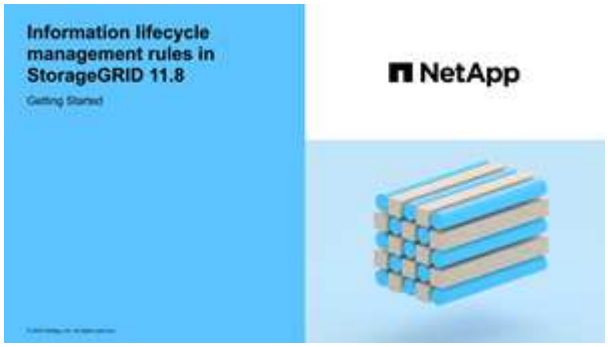
Use estas instruções para:

- Saiba mais sobre o StorageGRID ILM, incluindo"como o ILM opera ao longo da vida de um objeto" .
- Aprenda a configurar"pools de armazenamento" ,"Pools de armazenamento em nuvem" , e"Regras do ILM" .
- Aprenda como"criar, simular e ativar uma política de ILM" que protegerá dados de objetos em um ou mais sites.
- Aprenda como"gerenciar objetos com S3 Object Lock" , o que ajuda a garantir que objetos em buckets S3 específicos não sejam excluídos ou substituídos por um período de tempo especificado.

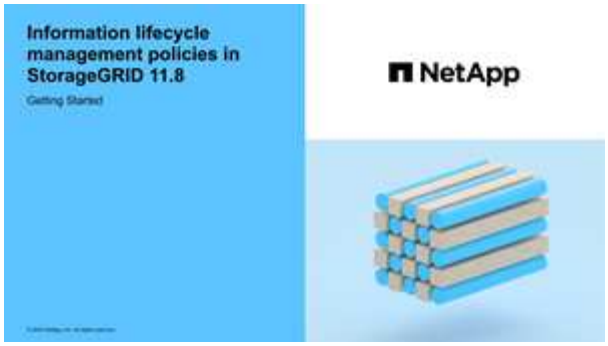
Saber mais

Para saber mais, assista a estes vídeos:

- "Vídeo: Visão geral das regras do ILM" .



- "Vídeo: Visão geral das políticas do ILM"



ILM e ciclo de vida do objeto

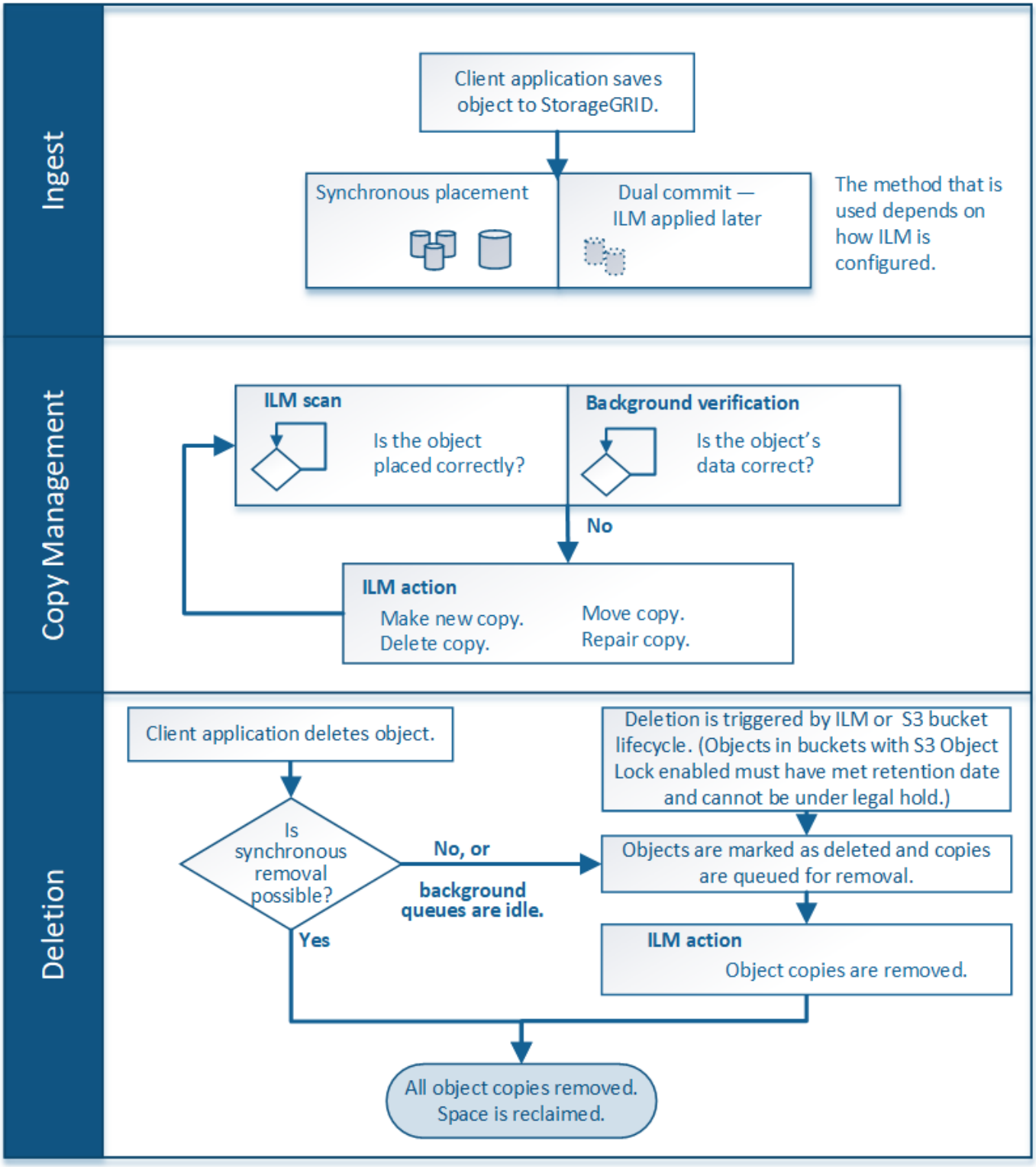
Como o ILM opera ao longo da vida de um objeto

Entender como o StorageGRID usa o ILM para gerenciar objetos durante cada estágio de sua vida útil pode ajudar você a criar uma política mais eficaz.

- **Ingestão**: A ingestão começa quando um aplicativo cliente S3 estabelece uma conexão para salvar um objeto no sistema StorageGRID e é concluída quando o StorageGRID retorna uma mensagem de "ingestão bem-sucedida" ao cliente. Os dados do objeto são protegidos durante a ingestão, aplicando instruções do ILM imediatamente (posicionamento síncrono) ou criando cópias provisórias e aplicando o ILM posteriormente (confirmação dupla), dependendo de como os requisitos do ILM foram especificados.
- **Gerenciamento de cópias**: Depois de criar o número e o tipo de cópias de objetos especificados nas instruções de posicionamento do ILM, o StorageGRID gerencia os locais dos objetos e os protege contra perdas.
  - **Varredura e avaliação do ILM**: O StorageGRID varre 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 cria automaticamente uma nova cópia do objeto ou um fragmento de objeto codificado para eliminação de substituição em um local que atenda aos requisitos atuais do ILM. Ver "Verificar integridade do objeto" .
- **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 uma exclusão por ILM ou exclusão causada pela expiração do ciclo de vida de um bucket do S3.

> ⓘ Objetos em um bucket que tenha o S3 Object Lock ativado não podem ser excluídos se estiverem sob retenção legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida.

O diagrama resume como o ILM opera durante todo o ciclo de vida de um objeto.



Como os objetos são ingeridos

Opções de ingestão

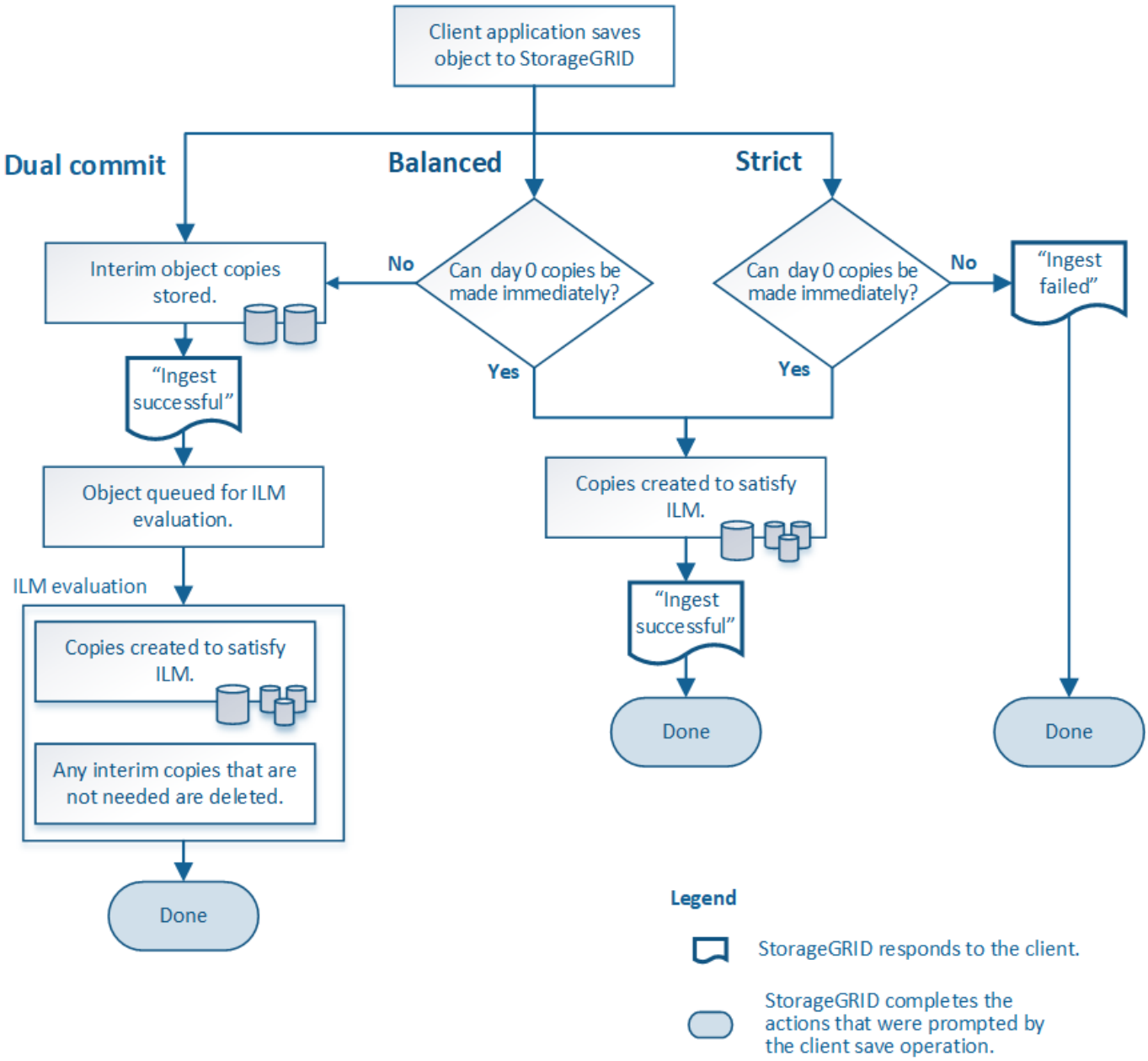
Ao criar uma regra de ILM, você especifica uma das três opções para proteger objetos na ingestão: Confirmação dupla, Estrita ou Balanceada.

Dependendo da sua escolha, o StorageGRID faz cópias provisórias e enfileira os objetos para avaliação

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

Fluxograma de opções de ingestão

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



Comprometimento duplo

Quando você seleciona a opção Dual commit, o StorageGRID imediatamente faz cópias provisórias do objeto em dois nós de armazenamento diferentes e retorna uma mensagem de "ingestão bem-sucedida" ao cliente. O objeto é enfileirado para avaliação do ILM, e cópias que atendem às instruções de posicionamento da regra são feitas posteriormente. Se a política ILM não puder ser processada imediatamente após a confirmação dupla, a proteção contra perda de site poderá levar algum tempo para ser alcançada.

Use a opção Dual commit em qualquer um destes casos:

- Você está usando regras de ILM multisite e a latência de ingestão do cliente é sua principal consideração. Ao usar o Dual Commit, você deve garantir que sua grade possa executar o trabalho adicional de criar e remover cópias de dual-commit se elas não satisfizerem o ILM. Especificamente:
  - A carga na rede deve ser baixa o suficiente para evitar um acúmulo de ILM.
  - A grade deve ter recursos de hardware excedentes (IOPS, CPU, memória, largura de banda de rede e assim por diante).
- Você está usando regras ILM multisite e a conexão WAN entre os sites geralmente tem alta latência ou largura de banda limitada. Nesse cenário, usar a opção Dual commit 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.

Equilibrado (padrão)

Quando você seleciona a opção Balanceado, 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 Strict, se o StorageGRID não puder fazer todas as cópias imediatamente, ele usará o Dual commit. Se a política de ILM usar posicionamentos em vários sites e a proteção imediata contra perda de site não puder ser alcançada, o alerta **posicionamento de ILM inalcançável** será acionado.

Use a opção Balanceado para obter a melhor combinação de proteção de dados, desempenho da grade e sucesso de ingestão. Balanceado é a opção padrão no assistente Criar regra ILM.

Estrito

Quando você seleciona a opção Estrito, 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 a operação novamente.

Use a opção Estrito se você tiver um requisito operacional ou regulatório para armazenar objetos imediatamente 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 Restrição de Localização para garantir que objetos nunca sejam armazenados em determinados data centers.

Ver "Exemplo 5: regras e política do ILM para comportamento de ingestão estrita" .

Vantagens, desvantagens e limitações das opções de ingestão

Entender as vantagens e desvantagens de cada uma das três opções para proteger dados na ingestão (balanceado, estrito ou confirmação dupla) pode ajudar você a decidir qual selecionar para uma regra de ILM.

Para uma visão geral das opções de ingestão, consulte"Opções de ingestão" .

Vantagens das opções Balanceada e Estrita

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

- **Melhor segurança de dados**: os dados do objeto são imediatamente protegidos, conforme especificado nas instruções de posicionamento da regra ILM, que podem ser configuradas para proteger contra uma ampla variedade de condições de falha, incluindo a falha de mais de um local de armazenamento. O commit duplo só pode proteger contra a perda de uma única cópia local.

- **Operação de grade mais eficiente**: Cada objeto é processado apenas uma vez, à medida que 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.
- **(Balanceado) Recomendado**: A opção Balanceada fornece eficiência ideal de ILM. É recomendável usar a opção Balanceado, a menos que o comportamento de ingestão Estrito seja necessário ou a grade atenda a todos os critérios para usar o Dual commit.
- **(Estrita) Certeza sobre localizações de objetos**: A opção Estrita garante que os objetos sejam armazenados imediatamente de acordo com as instruções de posicionamento na regra ILM.

Desvantagens das opções Balanceada e Estrita

Quando comparado ao Dual commit, as opções Balanced e Strict têm algumas desvantagens:

- **Ingestões de clientes mais longas**: As latências de ingestão de clientes podem ser maiores. Quando você usa as opções Balanceado ou Estrito, uma mensagem de "ingestão bem-sucedida" não é retornada ao cliente até que todos os fragmentos codificados para eliminação ou cópias replicadas sejam criados e armazenados. No entanto, os dados do objeto provavelmente chegarão ao seu posicionamento final muito mais rápido.
- **(Rigoroso) Taxas mais altas de falha de ingestão**: Com a opção Rigoroso, a ingestão falha sempre que o StorageGRID não consegue fazer imediatamente todas as cópias especificadas na regra ILM. Você poderá observar altas taxas de falha de ingestão se um local de armazenamento necessário estiver temporariamente offline ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(Rigoroso) Os posicionamentos de upload multipartes do S3 podem não ser como esperado em algumas circunstâncias**: Com o Rigoroso, você espera que os objetos sejam posicionados conforme descrito pela regra do ILM ou que a ingestão falhe. No entanto, com um upload multiparte do S3, o ILM é avaliado para cada parte do objeto à medida que ele é ingerido e para o objeto como um todo quando o upload multiparte é concluído. Nas seguintes circunstâncias, isso pode resultar em posicionamentos diferentes do esperado:
  - **Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento**: como cada parte é colocada de acordo com a regra que está ativa quando a parte é ingerida, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multiparte for 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 do ILM e movida para o local correto posteriormente.
  - **Quando as regras do ILM filtram por tamanho**: Ao avaliar o ILM para uma peça, o StorageGRID filtra pelo tamanho da peça, não pelo tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos do ILM para o objeto como um todo. Por exemplo, se uma regra especificar que todos os objetos de 10 GB ou maiores sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, na ingestão, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2. Quando o ILM é avaliado para o objeto, todas as partes do objeto são movidas para DC1.
- **(Rigoroso) A ingestão não falha quando tags de objeto ou metadados são atualizados e novos posicionamentos obrigatórios não podem ser feitos**: Com o Rigoroso, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. 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 do objeto acionadas pela atualização não são feitas imediatamente. Alterações de posicionamento são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano. Se as alterações de posicionamento necessárias não puderem ser feitas (por exemplo, porque um novo local necessário não está disponível), o objeto atualizado mantém seu posicionamento atual até que as alterações de posicionamento sejam possíveis.

Limitações no posicionamento de objetos com as opções Balanceado e Estrito

As opções Balanceado ou Estrito não podem ser usadas para regras ILM que tenham qualquer uma destas instruções de posicionamento:

- Colocação em um pool de armazenamento em nuvem no dia 0.
- Posicionamentos em um pool de armazenamento em nuvem quando a regra tem um horário de criação definido pelo usuário como seu horário de referência.

Essas restrições existem porque o StorageGRID não pode fazer cópias sincronizadas para um pool de armazenamento em nuvem, e um horário de criação definido pelo usuário pode ser resolvido para o presente.

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

Tanto sua regra ILM quanto sua escolha de consistência afetam 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 a consistência usada quando um objeto é armazenado afeta o posicionamento inicial de metadados de objetos. Como o StorageGRID requer acesso aos dados e metadados de um objeto para atender às solicitações do cliente, selecionar níveis correspondentes de proteção para consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas mais previsíveis do sistema.

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

- **Todos**: Todos os nós recebem metadados do objeto imediatamente ou a solicitação falhará.
- **Strong-global**: Os metadados do objeto são imediatamente distribuídos a todos os sites. Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site**: Os metadados do objeto são imediatamente distribuídos para outros nós no site. Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
- **Leitura após nova gravação**: fornece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.
- **Disponível**: Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .

> Antes de selecionar um valor de consistência,"leia a descrição completa de consistência" . Você deve entender os benefícios e limitações antes de alterar o valor padrão.

Exemplo de como a consistência e as regras do ILM podem interagir

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

- **Regra do ILM**: Crie duas cópias de objetos, uma no site local e outra em um site remoto. Use o comportamento de ingestão estrito.
- **consistência**: Forte-global (os metadados do objeto são imediatamente distribuídos para todos os sites).

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

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

Se, em vez disso, você usasse a mesma regra de ILM e a consistência de site forte, o cliente poderia receber uma mensagem de sucesso depois que os dados do objeto fossem replicados para o site remoto, mas antes que os metadados do objeto fossem distribuídos lá. Nesse caso, o nível de proteção dos metadados do objeto não corresponde ao nível de proteção dos dados do 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 consistência e regras de ILM pode ser complexa. Entre em contato com a NetApp se precisar de assistência.

Informações relacionadas

"Exemplo 5: regras e política do ILM para comportamento de ingestão estrita"

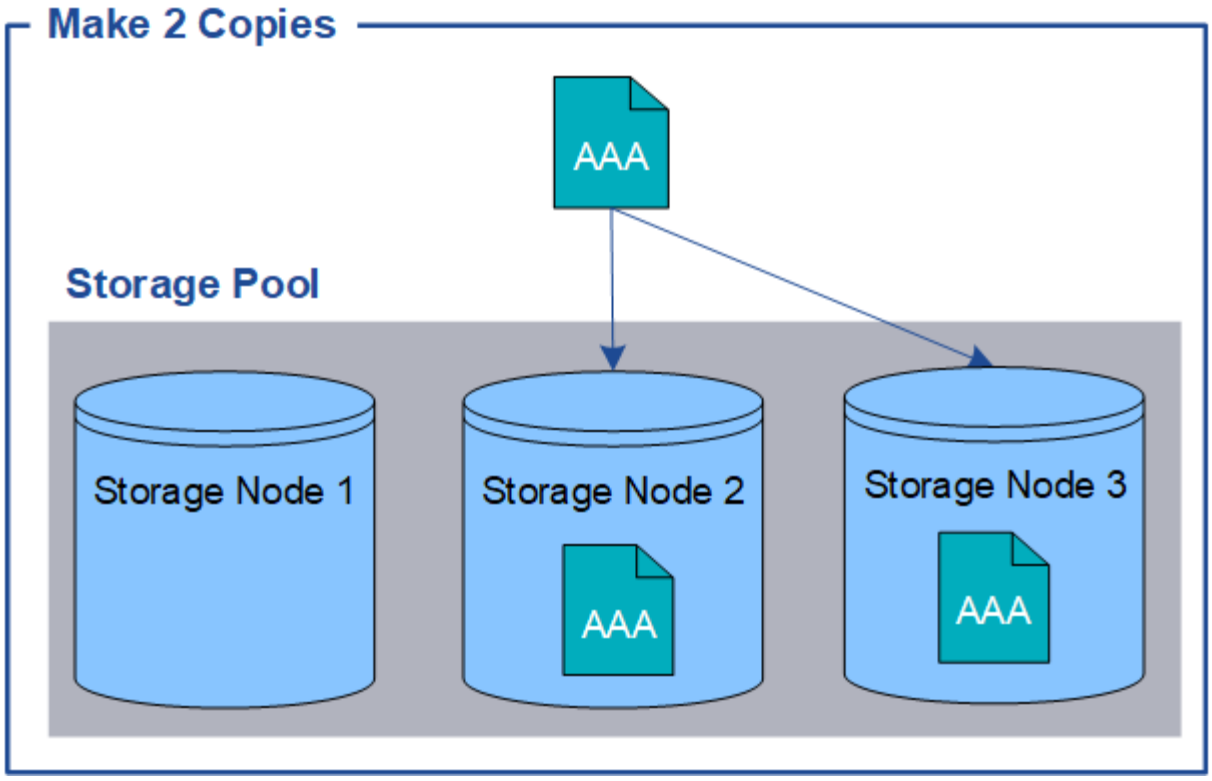
Como os objetos são armazenados (replicação ou codificação de eliminação)

O que é replicação?

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos (a codificação de eliminação é o outro método). Quando os objetos correspondem a uma regra do ILM que usa replicação, o sistema cria cópias exatas dos dados do objeto e armazena as cópias nos nós de armazenamento.

Ao configurar uma regra do ILM para criar cópias replicadas, você especifica quantas cópias devem ser criadas, onde elas devem ser colocadas e por quanto tempo elas devem ser armazenadas em cada local.

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



Quando o StorageGRID corresponde objetos a essa regra, ele cria duas cópias do objeto, colocando cada cópia em um nó de armazenamento diferente no pool de armazenamento. As duas cópias podem ser colocadas em quaisquer dois dos três nós de armazenamento disponíveis. Neste caso, a regra colocou cópias de objetos nos Nós de Armazenamento 2 e 3. Como há duas cópias, o objeto pode ser recuperado se algum dos nós no pool de armazenamento falhar.

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

Informações relacionadas

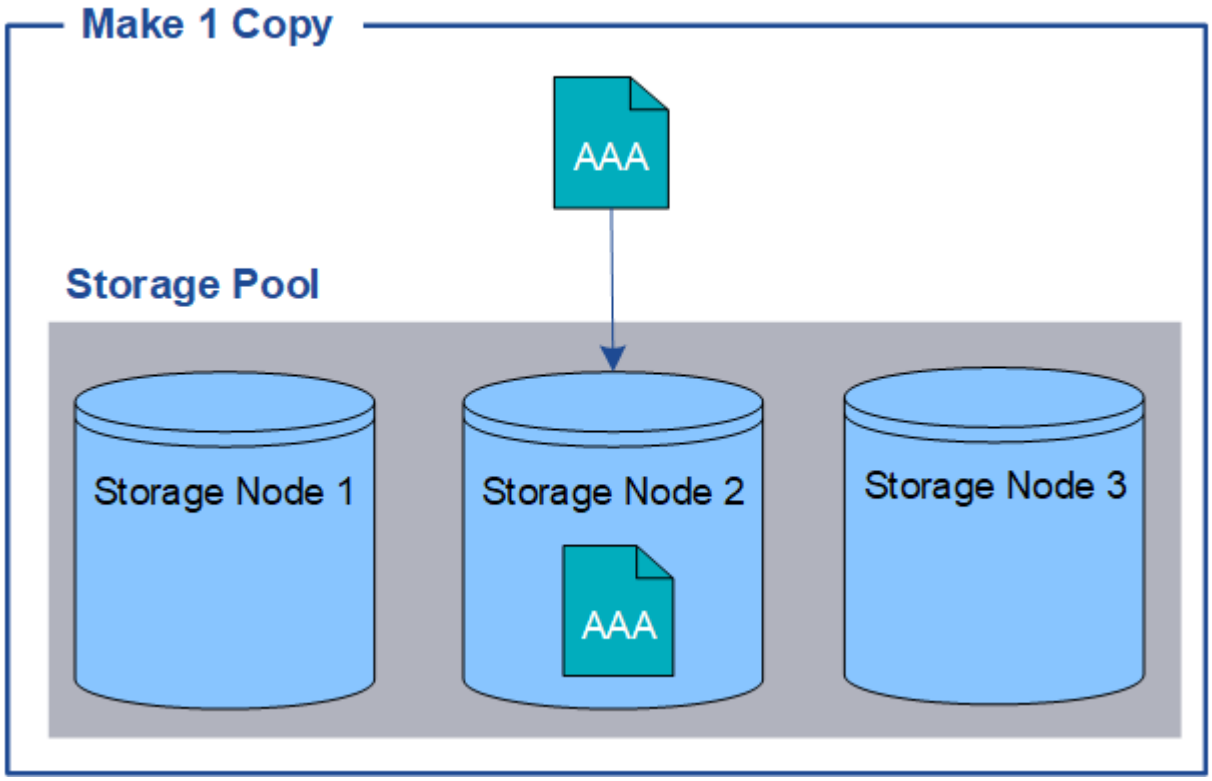
- "O que é codificação de apagamento"
- "O que é um pool de armazenamento"
- "Habilitar proteção contra perda de site usando replicação e codificação de eliminação"

Por que você não deve usar replicação de cópia única

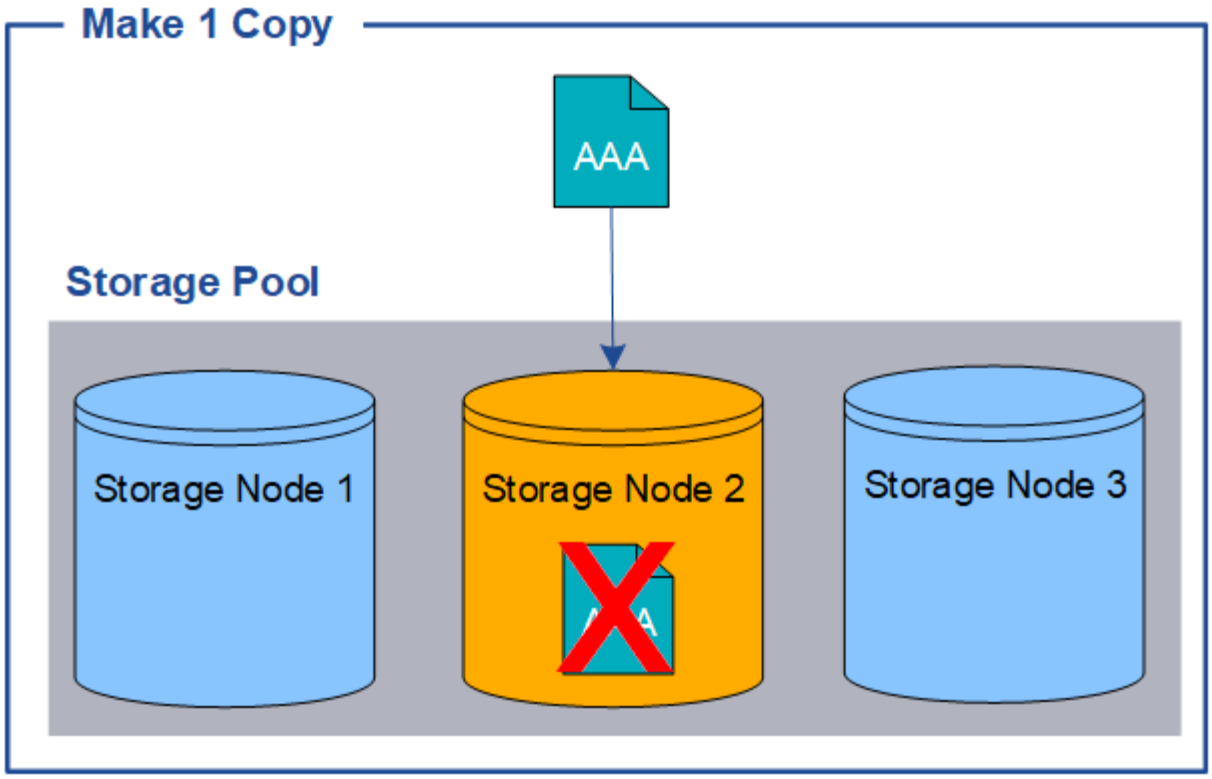
Ao criar uma regra de ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de posicionamento.

> Não use uma regra de ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se existir 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.

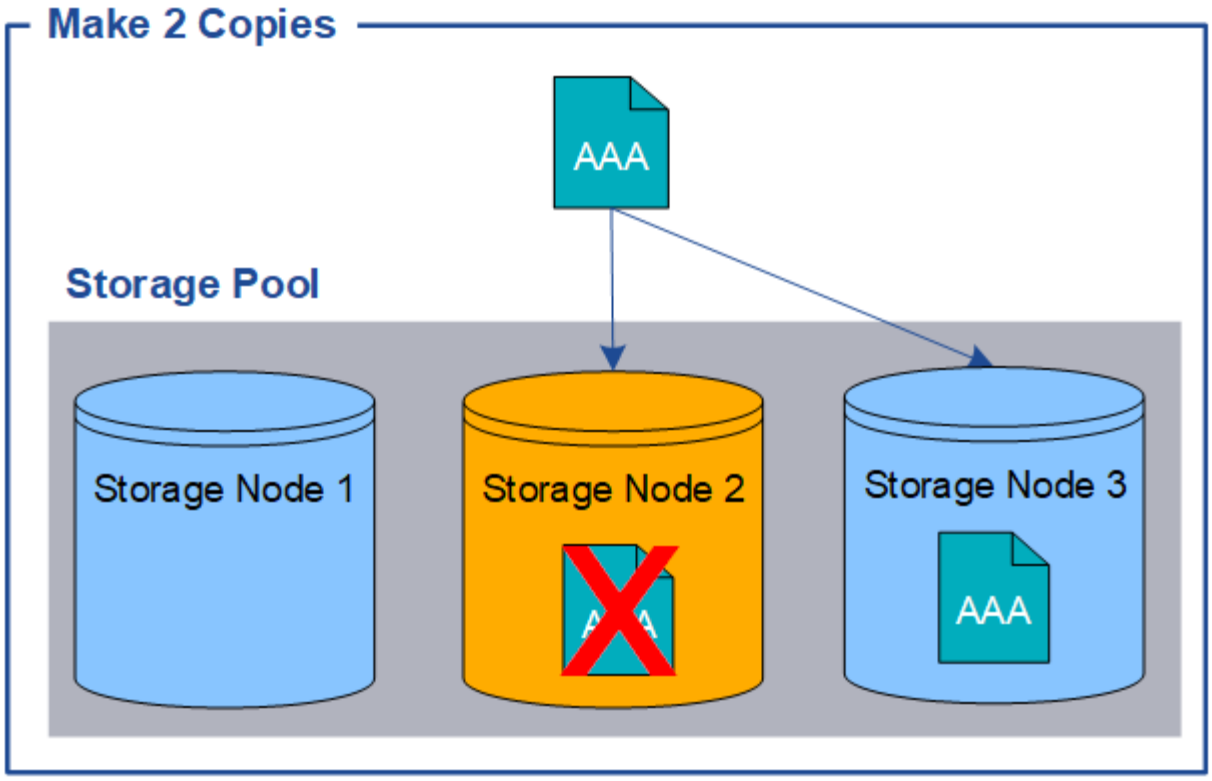
No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de armazenamento que contém três nós de armazenamento. Quando um objeto que corresponde a essa regra é ingerido, o StorageGRID coloca uma única cópia em apenas um nó de armazenamento.



Quando uma regra de ILM cria apenas uma cópia replicada de um objeto, o objeto se torna 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 completamente se o Nó de Armazenamento 2 falhar.



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



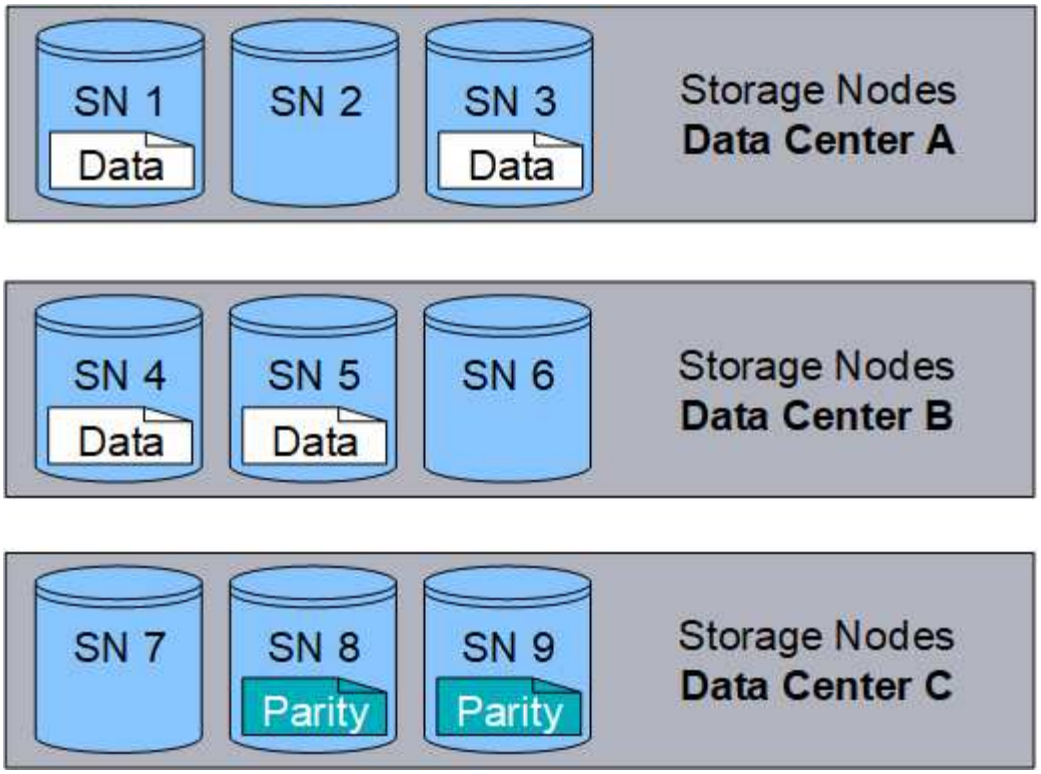
O que é codificação de eliminação?

A codificação de eliminação é um dos dois métodos que o StorageGRID usa para armazenar dados de objetos (a replicação é o outro método). Quando objetos correspondem a uma regra ILM que usa codificação de eliminação, esses objetos são divididos em fragmentos de dados, fragmentos de paridade adicionais são computados e cada fragmento é armazenado em um nó de armazenamento diferente.

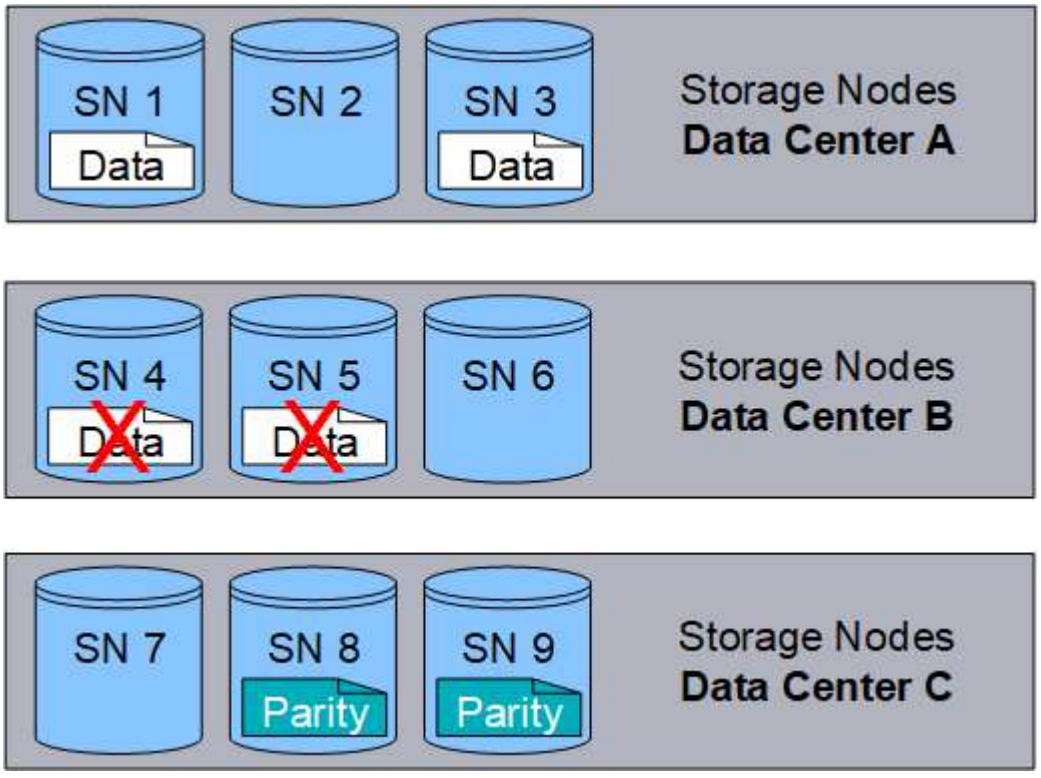
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade for corrompido ou perdido, o algoritmo de codificação de eliminação pode recriar esse fragmento usando um subconjunto dos dados e fragmentos de paridade restantes.

À medida que você cria regras de ILM, o StorageGRID cria perfis de codificação de eliminação que dão suporte a essas regras. Você pode visualizar uma lista de perfis de codificação de eliminação,"renomear um perfil de codificação de eliminação" , ou"desativar um perfil de codificação de eliminação se ele não estiver sendo usado atualmente em nenhuma regra do ILM" .

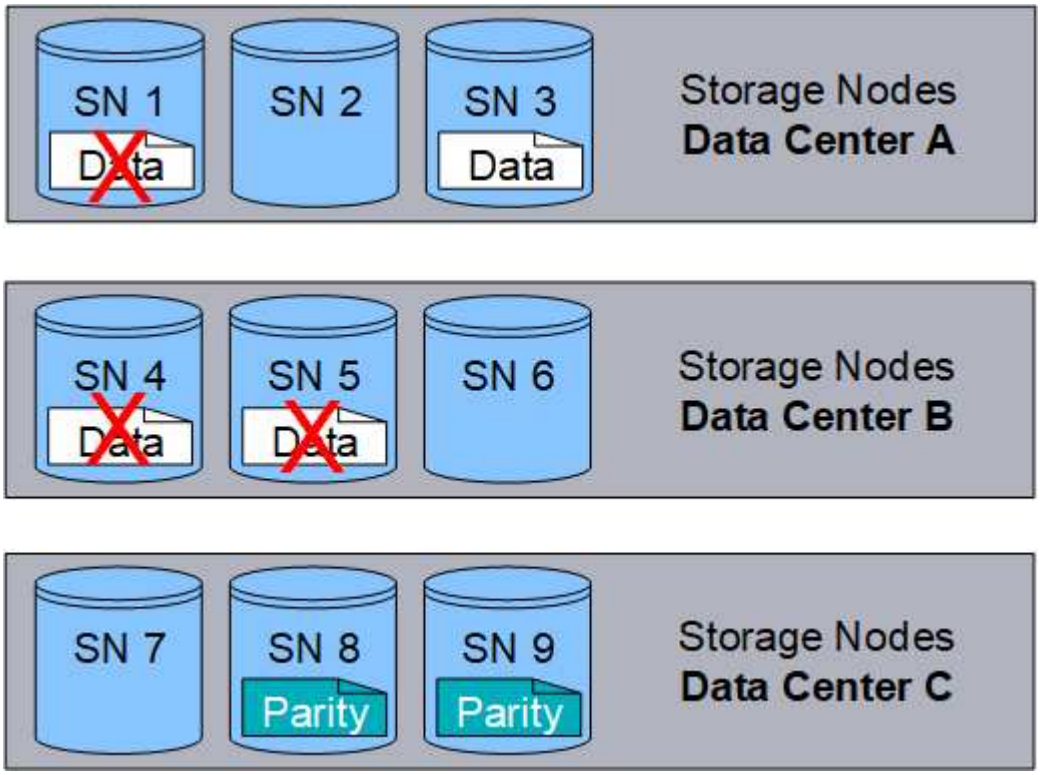
O exemplo a seguir ilustra o uso de um algoritmo de codificação de eliminação nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de eliminação 4+2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados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



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



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



Informações relacionadas

- "O que é replicação"
- "O que é um pool de armazenamento"
- "O que são esquemas de codificação de apagamento"
- "Renomear um perfil de codificação de eliminação"
- "Desativar um perfil de codificação de eliminação"

O que são esquemas de codificação de apagamento?

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

Ao criar ou editar uma regra ILM, você seleciona um esquema de codificação de eliminação disponível. O StorageGRID cria automaticamente esquemas de codificação de eliminação com base em quantos nós de armazenamento e sites compõem o pool de armazenamento que você planeja usar.

Proteção de dados

O sistema StorageGRID usa o algoritmo de codificação de eliminação Reed-Solomon. O algoritmo divide um objeto em `k` fragmentos de dados e cálculos `m` fragmentos de paridade.

O `k + m = n` fragmentos estão espalhados por `n` Nós de armazenamento para fornecer proteção de dados da seguinte forma:

- Para recuperar ou reparar um objeto, `k` fragmentos são necessários.
- Um objeto pode sustentar até `m` fragmentos perdidos ou corrompidos. Quanto maior o valor de `m` , maior

será a tolerância a falhas.

A melhor proteção de dados é fornecida pelo esquema de codificação de eliminação com a maior tolerância a falhas de nó ou volume dentro de um pool de armazenamento.

Despesas gerais de armazenamento

A sobrecarga de armazenamento de um esquema de codificação de eliminação é calculada dividindo o número de fragmentos de paridade(`m`) pelo número de fragmentos de dados(`k`). Você pode usar a sobrecarga de armazenamento para calcular quanto espaço em disco cada objeto codificado por eliminação 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 consumirá 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 consumirá aproximadamente 13,3 MB.

Selecione o esquema de codificação de apagamento com o menor valor total de `k+m` que atenda às suas necessidades. Esquemas de codificação de apagamento com um número menor de fragmentos são mais eficientes computacionalmente porque:

- Menos fragmentos são criados e distribuídos (ou recuperados) por objeto
- Eles apresentam melhor desempenho porque o tamanho do fragmento é maior
- Eles podem exigir que menos nós sejam adicionados em um"expansão quando mais armazenamento é necessário"

Diretrizes para pools de armazenamento

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

- O pool de armazenamento deve incluir três ou mais sites, ou exatamente um site.

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

  - Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites
  - Esquemas de codificação de eliminação para pools de armazenamento de um site
- Não use um pool de armazenamento que inclua o site Todos os Sites.
- O pool de armazenamento deve incluir pelo menos *`k+m`* `+1` Nós de armazenamento que podem armazenar dados de objetos.

  > Os nós de armazenamento podem ser configurados durante a instalação para conter apenas metadados de objetos e não dados de objetos. Para obter mais informações, consulte "Tipos de nós de armazenamento" .

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

Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites

A tabela a seguir descreve os esquemas de codificação de eliminação atualmente suportados pelo StorageGRID para pools de armazenamento que incluem três ou mais sites. Todos esses esquemas oferecem proteção contra perda de local. Um site pode ser perdido, e o objeto ainda estará acessível.

Para esquemas de codificação de eliminação que fornecem proteção contra perda de site, o número recomendado de nós de armazenamento no pool de armazenamento excede `k+m +1` porque cada site requer um mínimo de três nós de armazenamento.

Esquema de codificação de apagamento (*k+m*)	Número mínimo de sites implantados	Número recomendado de nós de armazenamento em cada site	Número total recomendado de nós de armazenamento	Proteção contra perda de site?	Despesas gerais de armazenamento
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%
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 no mínimo três nós de armazenamento por site. Para usar o esquema 7+5, cada site requer um mínimo de quatro nós de armazenamento. É recomendável usar cinco nós de armazenamento por site.

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

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

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

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

Esquemas de codificação de eliminação para pools de armazenamento de um site

Um pool de armazenamento de um site suporta todos os esquemas de codificação de eliminação definidos para três ou mais sites, desde que o site tenha nós de armazenamento suficientes.

O número mínimo de nós de armazenamento necessários é `k+m` , mas um pool de armazenamento com `k+m +1` Nós de armazenamento são recomendados. Por exemplo, o esquema de codificação de eliminação 2+1 requer um pool de armazenamento com no mínimo três nós de armazenamento, mas quatro nós de armazenamento são recomendados.

Esquema de codificação de apagamento (*k+m*)	Número mínimo de nós de armazenamento	Número recomendado de nós de armazenamento	Despesas gerais de armazenamento
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Vantagens, desvantagens e requisitos para codificação de apagamento

Antes de decidir se deve usar replicação ou codificação de eliminação para proteger dados de objetos contra perda, você deve entender as vantagens, desvantagens e os requisitos da codificação de eliminação.

Vantagens da codificação de apagamento

Quando comparado à replicação, a codificação de eliminação oferece maior confiabilidade, disponibilidade e

eficiência de armazenamento.

- **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 diferentes nós e entre sites. Com a codificação de eliminação, um objeto é codificado em dados e fragmentos de paridade e distribuído entre muitos nós e sites. Essa dispersão fornece proteção contra falhas no local e no nó. Quando comparado à replicação, a codificação de eliminação proporciona maior confiabilidade com custos de armazenamento comparáveis.
- **Disponibilidade**: Disponibilidade pode ser definida como a capacidade de recuperar objetos se os Nós de Armazenamento falharem ou se tornarem inacessíveis. Quando comparado à replicação, a codificação de eliminação proporciona maior disponibilidade a custos de armazenamento comparáveis.
- **Eficiência de armazenamento**: Para níveis semelhantes de disponibilidade e confiabilidade, objetos protegidos por codificação de eliminação consomem menos espaço em disco do que os mesmos objetos se protegidos por replicação. Por exemplo, um objeto de 10 MB replicado em dois sites consome 20 MB de espaço em disco (duas cópias), enquanto um objeto codificado por eliminação em três sites com um esquema de codificação por eliminação 6+3 consome apenas 15 MB de espaço em disco.

> ⓘ O espaço em disco para objetos codificados para eliminação é calculado como o tamanho do objeto mais a sobrecarga de armazenamento. A porcentagem de sobrecarga de armazenamento é o número de fragmentos de paridade dividido pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Quando comparado à replicação, a codificação de eliminação tem as seguintes desvantagens:

- Recomenda-se um número maior de nós de armazenamento e sites, dependendo do esquema de codificação de eliminação. Por outro lado, se você replicar dados de objeto, precisará apenas de um nó de armazenamento para cada cópia. Ver"Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites" e"Esquemas de codificação de eliminação para pools de armazenamento de um site" .
- Aumento de custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, adicione capacidade de armazenamento em cada local onde as cópias de objetos são feitas. Para expandir uma implantação que usa codificação de eliminação, você deve considerar o esquema de codificação de eliminação em uso e o quão cheios os nós de armazenamento existentes estão. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, você deve adicionar pelo menos `k+m` Nós de armazenamento, mas se você expandir quando os nós existentes estiverem 70% cheios, você pode adicionar dois nós por site e ainda maximizar a capacidade de armazenamento utilizável. Para obter mais informações, consulte "Adicionar capacidade de armazenamento para objetos codificados por eliminação" .
- Há latências de recuperação maiores quando você usa codificação de eliminação em sites distribuídos geograficamente. Os fragmentos de objeto de um objeto codificado por eliminação e distribuído em sites remotos demoram mais para serem recuperados por meio de conexões WAN do que um objeto replicado e disponível localmente (o mesmo site ao qual o cliente se conecta).
- Ao usar codificação de eliminação 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 eliminação em vários sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência da rede entre os sites aumenta. Essa diminuição se deve à diminuição correspondente na taxa de transferência da rede TCP, que afeta a rapidez com que o sistema StorageGRID pode armazenar e recuperar fragmentos de objetos.

- Maior uso de recursos de computação.

Quando usar codificação de apagamento

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

- Objetos com tamanho maior que 1 MB.

> A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

- Armazenamento a longo prazo ou a frio para conteúdo recuperado com pouca frequência.
- Alta disponibilidade e confiabilidade de dados.
- Proteção contra falhas completas de sites e nós.
- Eficiência de armazenamento.
- Implantações de site único que exigem proteção de dados eficiente com apenas uma única cópia codificada para eliminação, em vez de várias cópias replicadas.
- Implantações em vários sites onde a latência entre sites é inferior a 100 ms.

Como a retenção de objetos é determinada

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

Como os usuários locatários controlam a retenção de objetos

Os usuários locatários podem usar estes métodos para controlar por quanto tempo seus objetos são armazenados no StorageGRID:

- Se a configuração global do Bloqueio de Objeto S3 estiver habilitada para a grade, os usuários do locatário S3 poderão criar buckets com o Bloqueio de Objeto S3 habilitado e, em seguida, selecionar um **Período de retenção padrão** para cada bucket.
- Se a configuração global de Bloqueio de Objeto do S3 estiver habilitada para a grade, os usuários do locatário do S3 poderão criar buckets com o Bloqueio de Objeto do S3 habilitado e, em seguida, usar a API REST do S3 para especificar as configurações de retenção até a data e retenção legal para cada versão de objeto adicionada a esse bucket.
  - Uma versão de objeto que está sob retenção legal não pode ser excluída por nenhum método.
  - Antes que a data de retenção de uma versão do objeto seja atingida, essa versão não pode ser excluída por nenhum método.
  - Objetos em buckets com o S3 Object Lock habilitado são retidos pelo ILM "para sempre". No entanto, após atingir a data de retenção, uma versão do objeto pode ser excluída por uma solicitação do cliente ou pela expiração do ciclo de vida do bucket. Ver "Gerenciar objetos com o S3 Object Lock" .
- Os usuários do locatário do S3 podem adicionar uma configuração de ciclo de vida aos seus buckets que especifica uma ação de expiração. Se houver um ciclo de vida de bucket, o StorageGRID armazenará um objeto até que a data ou o número de dias especificado na ação Expiração sejam atingidos, a menos que

o cliente exclua o objeto primeiro. Ver "Criar configuração do ciclo de vida do S3" .

- Um cliente S3 pode emitir uma solicitação de exclusão de objeto. O StorageGRID sempre prioriza as solicitações de exclusão do cliente em relação ao ciclo de vida do bucket S3 ou ILM ao determinar se um objeto deve ser excluído ou mantido.

Como os administradores de grade controlam a retenção de objetos

Os administradores de grade podem usar estes métodos para controlar a retenção de objetos:

- Defina um período máximo de retenção do bloqueio de objeto S3 para cada locatário. Em seguida, os usuários locatários podem definir um período de retenção padrão para cada um de seus buckets. O período máximo de retenção também é aplicado a quaisquer objetos recém-ingeridos para esse bucket (data de retenção do objeto).
- Crie instruções de posicionamento do ILM para controlar por quanto tempo os objetos são armazenados. Quando 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 retidos indefinidamente se "para sempre" for especificado nas instruções de posicionamento.
- 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 eliminação) são armazenadas e onde as cópias estão localizadas (nós de armazenamento ou pools de armazenamento em nuvem).

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

Quando um ciclo de vida de bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro do ciclo de vida. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções do ILM para posicioná-lo tenham expirado.

Exemplos de retenção de objetos

Para entender melhor as interações entre o bloqueio de objeto do 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 os objetos por mais tempo que o ILM

ILM

Armazene duas cópias por 1 ano (365 dias)

Ciclo de vida do bucket

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 um objeto deve ser excluído ou mantido.

> ⓘ 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 posicionamento do ILM ao determinar o número e o tipo de cópias a serem armazenadas. Neste exemplo, duas cópias do objeto continuarão armazenadas no StorageGRID dos dias 366 a 730.

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

ILM

Armazene duas cópias por 2 anos (730 dias)

Ciclo de vida do bucket

Expirar 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

Armazene duas cópias nos nós de armazenamento "para sempre"

Ciclo de vida do bucket

Expira objetos em 2 anos (730 dias)

Solicitação de exclusão de 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: O bloqueio de objeto S3 substitui a solicitação de exclusão do cliente

Bloqueio de Objeto S3

A data de retenção para uma versão de objeto é 31/03/2026. Uma retenção legal não está em vigor.

Regra ILM compatível

Armazene duas cópias nos nós de armazenamento "para sempre"

Solicitação de exclusão de cliente

Emitido em 31/03/2024

Resultado

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

Como os objetos são excluídos

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

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

- Exclusão síncrona: quando o StorageGRID recebe uma solicitação de exclusão do cliente, todas as cópias do objeto são removidas imediatamente. O cliente é informado de que a exclusão foi bem-sucedida após as cópias serem 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 que a exclusão foi bem-sucedida. Cópias de objetos são removidas posteriormente pelo processamento ILM em segundo plano.

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

A tabela resume quando o StorageGRID usa cada método.

Método de execução da exclusão	Quando usado
Os objetos são colocados 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 foi atingido. ◦ O último período de tempo especificado em uma regra ILM expirou. **Observação:** Objetos em um bucket que tenha o Bloqueio de Objeto S3 habilitado não podem ser excluídos se estiverem sob retenção legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida. • Um cliente S3 solicita exclusão e uma ou mais destas condições são verdadeiras: ◦ As cópias não podem ser excluídas em 30 segundos porque, por exemplo, a localização de um objeto está temporariamente indisponível. ◦ As filas de exclusão em segundo plano estão ociosas.
Os objetos são removidos imediatamente (exclusão síncrona)	Quando um cliente S3 faz uma solicitação de exclusão e **todas** as seguintes condições são atendidas: • Todas as cópias podem ser removidas em 30 segundos. • As filas de exclusão em segundo plano contêm objetos a serem processados.

Quando clientes S3 fazem solicitações de exclusão, o StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, ele alterna para executar a exclusão síncrona. Garantir que a fila de exclusão em segundo plano tenha 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 evitar atrasos na exclusão de clientes.

Tempo necessário para excluir objetos

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

- Quando o StorageGRID executa uma exclusão síncrona, pode levar até 30 segundos para o StorageGRID 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 enfileira objetos para exclusão.

- Se você estiver monitorando de perto o desempenho da exclusão durante uma exclusão em massa, poderá notar que a taxa de exclusão parece ficar lenta depois que um certo número de objetos é excluído. Essa alteração ocorre quando o StorageGRID muda de enfileiramento de objetos para exclusão para execução de exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias de objetos estão sendo removidas mais lentamente. Pelo contrário, indica que, em média, o espaço está sendo liberado mais rapidamente.

Se você estiver excluindo um grande número de objetos e sua prioridade for liberar espaço rapidamente, considere usar uma solicitação do 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.

O tempo necessário para liberar espaço após a exclusão de um objeto depende de vários fatores:

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

Como objetos versionados do 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, independentemente de essas solicitações virem de um cliente S3, da expiração do ciclo de vida de um bucket do S3 ou dos 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 liberam espaço. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão de zero byte como a versão atual do objeto, o que torna a versão anterior do objeto "não atual". Um marcador de exclusão de objeto se torna um marcador de exclusão de objeto expirado quando é a versão atual e não há versões não atuais.

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. Entretanto, como os dados do objeto não atual não foram removidos, as solicitações que especificam uma versão não atual do objeto podem ser bem-sucedidas.

Para liberar espaço ao excluir objetos versionados ou para remover marcadores de exclusão, use um dos seguintes:

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

  O `NewerNoncurrentVersions` ação na configuração do ciclo de vida do bucket especifica o número de versões não atuais retidas em um bucket S3 versionado. Se houver mais versões não atuais do que `NewerNoncurrentVersions` especifica que o StorageGRID remove as versões mais antigas quando o valor NoncurrentDays tiver decorrido. O `NewerNoncurrentVersions` O limite substitui as regras do

ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do `NewerNoncurrentVersions` o limite é mantido se o ILM solicitar sua exclusão.

Para remover marcadores de exclusão de objetos expirados, use o `Expiration` ação com uma das seguintes tags: `ExpiredObjectDeleteMarker` , `Days` , ou `Date` .

- **ILM**:"Clonar uma política ativa" e adicionar duas regras ILM à nova política:
  - Primeira regra: use "Horário não atual" como o horário de referência para corresponder às versões não atuais do objeto. Em"Etapa 1 (Inserir detalhes) do assistente Criar uma regra ILM" , selecione **Sim** para a pergunta "Aplicar esta regra somente a versões mais antigas de objetos (em buckets do S3 com controle de versão habilitado)?"
  - Segunda regra: use **Tempo de ingestão** para corresponder à versão atual. A regra "Tempo não atual" deve aparecer na política acima da regra **Tempo de ingestão**.

    Para remover marcadores de exclusão de objetos expirados, use uma regra de **Tempo de ingestão** para corresponder aos marcadores de exclusão atuais. Os marcadores de exclusão são removidos somente quando um **período de tempo** de **dias** tiver passado e o criador de exclusão atual tiver expirado (não há versões não atuais).
- **Excluir objetos no bucket**: Use o gerenciador de inquilinos para"excluir todas as versões do objeto" , incluindo marcadores de exclusão, de um bucket.

Quando um objeto versionado é excluído, o StorageGRID cria um marcador de exclusão de zero byte como a versão atual do objeto. Todos os objetos e marcadores de exclusão devem ser removidos antes que um bucket versionado possa ser excluído.

- Os marcadores de exclusão criados no StorageGRID 11.7 ou anterior só podem ser removidos por meio de solicitações do cliente S3; eles não são removidos pelo ILM, pelas regras do ciclo de vida do bucket ou por objetos de exclusão em operações de bucket.
- Os marcadores de exclusão de um bucket criado no StorageGRID 11.8 ou posterior podem ser removidos por ILM, regras de ciclo de vida do bucket, objetos de exclusão em operações de bucket ou uma exclusão explícita do cliente S3.

Informações relacionadas

- "Usar API REST do S3"
- "Exemplo 4: regras e políticas do ILM para objetos versionados do S3"

Criar e atribuir níveis de armazenamento

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

Quando você instala o StorageGRID pela primeira vez, o nível de armazenamento **Padrão** é atribuído automaticamente a cada Nó de Armazenamento no seu sistema. Conforme necessário, você pode definir

opcionalmente níveis de armazenamento personalizados e atribuí-los a diferentes nós de armazenamento.

O uso de níveis de armazenamento personalizados permite que você crie pools de armazenamento ILM que contêm apenas um tipo específico de nó de armazenamento. Por exemplo, você pode querer que determinados objetos sejam armazenados em seus nós de armazenamento mais rápidos, como os dispositivos de armazenamento all-flash StorageGRID .

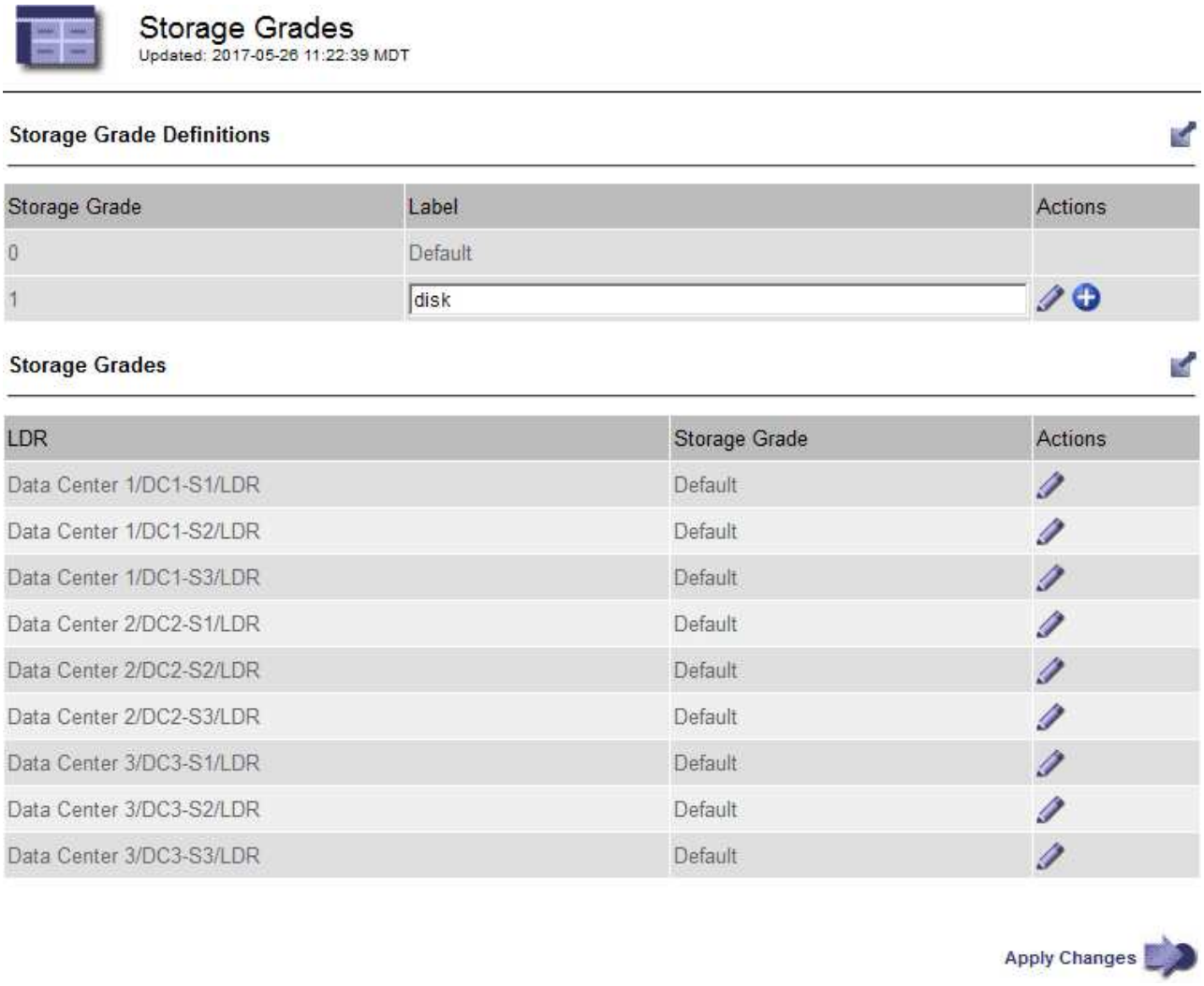
> Os nós de armazenamento podem ser configurados durante a instalação para conter apenas metadados de objetos e não dados de objetos. Nós de armazenamento somente de metadados não podem receber uma classificação de armazenamento. Para obter mais informações, consulte "Tipos de nós de armazenamento" .

Se o grau de armazenamento não for uma preocupação (por exemplo, todos os nós de armazenamento forem idênticos), você pode pular este procedimento e usar a seleção **inclui todos os graus de armazenamento** para o grau de armazenamento quando você"criar pools de armazenamento" . Usar essa seleção garante que o pool de armazenamento incluirá todos os nós de armazenamento no site, independentemente do seu nível de armazenamento.

> Não crie mais níveis de armazenamento do que o necessário. Por exemplo, não crie um nível de armazenamento para cada nó de armazenamento. Em vez disso, atribua cada grau de armazenamento a dois ou mais nós. Os níveis de armazenamento atribuídos a apenas um nó podem causar atrasos no ILM se esse nó ficar indisponível.

Passos

1. Selecione **ILM** > **Níveis de armazenamento**.
2. Defina níveis de armazenamento personalizados:
   a. Para cada nível de armazenamento personalizado que você deseja adicionar, selecione *Inserir* para adicionar uma linha.
   b. Insira um rótulo descritivo.



c. Selecione **Aplicar alterações**.

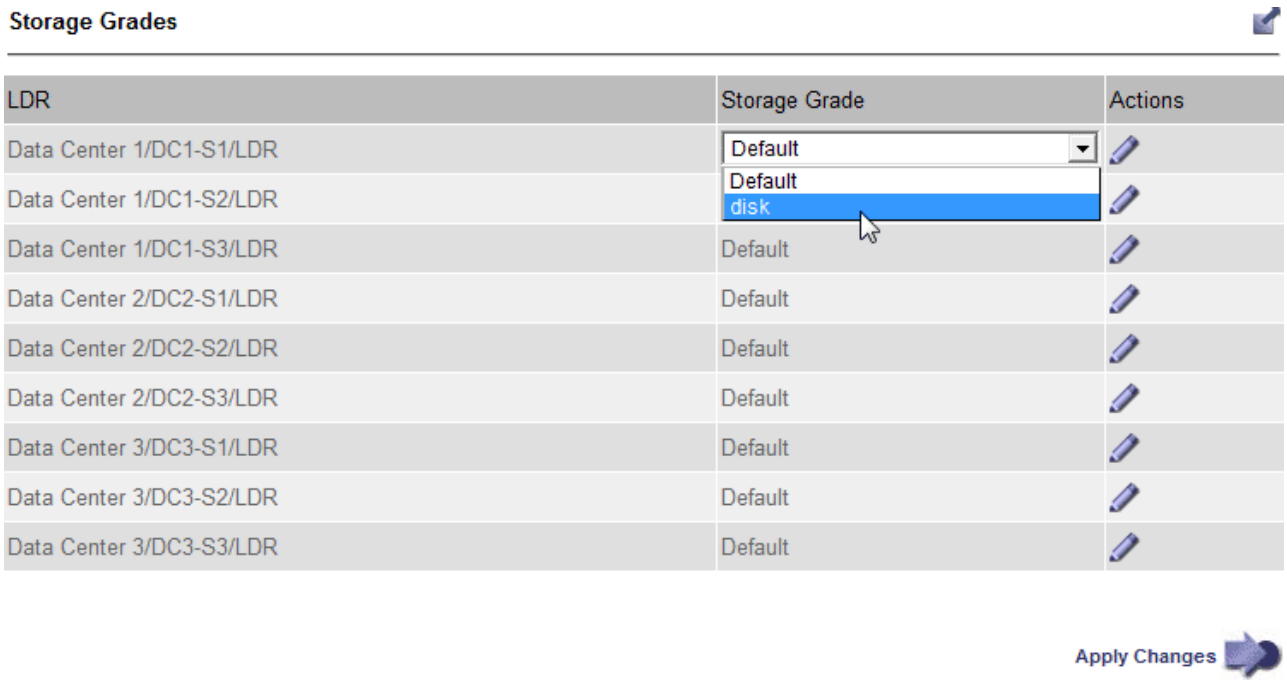
d. Opcionalmente, se você precisar modificar um rótulo salvo, selecione **Editar*** e selecione ***Aplicar alterações**.

Você não pode excluir notas de armazenamento.

3. Atribuir novos níveis de armazenamento aos nós de armazenamento:

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

b. Selecione o nível de armazenamento apropriado na lista.



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

a. Selecione **Aplicar alterações**.

Use pools de armazenamento

O que é um pool de armazenamento?

Um pool de armazenamento é um agrupamento lógico de nós de armazenamento.

Quando você instala o StorageGRID, um pool de armazenamento por site é criado automaticamente. Você pode configurar pools de armazenamento adicionais conforme necessário para suas necessidades de armazenamento.

> Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados de objetos, ou apenas metadados de objetos. Nós de armazenamento somente de metadados não podem ser usados em pools de armazenamento. Para obter mais informações, consulte "Tipos de nós de armazenamento" .

Os pools de armazenamento têm dois atributos:

- **Grau de armazenamento**: Para nós de armazenamento, o desempenho relativo do armazenamento de suporte.
- **Local**: O data center onde os objetos serão armazenados.

Pools de armazenamento são usados em regras de ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar regras de ILM para replicação, você seleciona

um ou mais pools de armazenamento.

Diretrizes para criação de pools de armazenamento

Configure e use pools de armazenamento para proteger contra perda de dados distribuindo dados entre vários sites. Cópias replicadas e cópias codificadas para eliminação exigem configurações de pool de armazenamento diferentes.

Ver "Exemplos de ativação da proteção contra perda de site usando replicação e codificação de eliminação" .

Diretrizes para todos os pools de armazenamento

- Mantenha as configurações do pool de armazenamento o mais simples possível. Não crie mais pools de armazenamento do que o necessário.
- Crie pools de armazenamento com o maior número possível de nós. Cada pool de armazenamento deve conter dois ou mais nós. Um pool de armazenamento com nós insuficientes pode causar atrasos no ILM se um nó ficar indisponível.
- Evite criar ou usar pools de armazenamento que se sobreponham (contenham um ou mais nós iguais). Se os pools de armazenamento se sobrepuserem, mais de uma cópia dos dados do objeto poderá ser salva no mesmo nó.
- Em geral, não use o pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) ou o site All Sites. Esses itens são atualizados automaticamente para incluir quaisquer novos sites que você adicionar em uma expansão, o que pode não ser o comportamento desejado.

Diretrizes para pools de armazenamento usados para cópias replicadas

- Para proteção contra perda de site usando"replicação" , especifique um ou mais pools de armazenamento específicos do site no"instruções de posicionamento para cada regra ILM" .

  Um pool de armazenamento é criado automaticamente para cada site durante a instalação do StorageGRID .

  Usar um pool de armazenamento para cada site garante que cópias de objetos replicadas sejam colocadas exatamente onde você espera (por exemplo, uma cópia de cada objeto em cada site para proteção contra perda de site).

- Se você adicionar um site em uma expansão, crie um novo pool de armazenamento que contenha somente o novo site. Então,"atualizar regras do ILM" para controlar quais objetos são armazenados no novo site.
- Se o número de cópias for menor que o número de pools de armazenamento, o sistema distribuirá as cópias para equilibrar o uso do disco entre os pools.
- Se os pools de armazenamento se sobrepuserem (contiverem os mesmos nós de armazenamento), todas as cópias do objeto poderão ser salvas em apenas um site. Você deve garantir que os pools de armazenamento selecionados não contenham os mesmos nós de armazenamento.

Diretrizes para pools de armazenamento usados para cópias codificadas por eliminação

- Para proteção contra perda de site usando"codificação de apagamento" , crie pools de armazenamento que consistam em pelo menos três sites. Se um pool de armazenamento incluir apenas dois sites, você não poderá usá-lo para codificação de eliminação. Não há esquemas de codificação de eliminação disponíveis para um pool de armazenamento com dois sites.

- O número de nós de armazenamento e sites contidos no pool de armazenamento determinam quais"esquemas de codificação de apagamento" estão disponíveis.
- Se possível, um pool de armazenamento deve incluir mais do que o número mínimo de nós de armazenamento necessários para o esquema de codificação de eliminação selecionado. Por exemplo, se você usar um esquema de codificação de eliminação 6+3, deverá ter pelo menos nove nós de armazenamento. No entanto, é recomendável ter pelo menos um nó de armazenamento adicional por site.
- Distribua os nós de armazenamento entre os sites da maneira mais uniforme possível. Por exemplo, para dar suporte a um esquema de codificação de eliminação 6+3, configure um pool de armazenamento que inclua pelo menos três nós de armazenamento em três sites.
- Se você tiver requisitos de alta taxa de transferência, não é recomendável usar um pool de armazenamento que inclua vários sites se a latência da rede entre os sites for maior que 100 ms. À medida que a latência aumenta, a taxa na qual o StorageGRID pode criar, posicionar e recuperar fragmentos de objetos diminui drasticamente devido à diminuição na taxa de transferência da rede TCP.

  A redução na taxa de transferência afeta as taxas máximas alcançáveis de ingestão e recuperação de objetos (quando Balanceado ou Estrito são selecionados como comportamento de ingestão) ou pode levar a pendências na fila do ILM (quando Confirmação dupla é selecionado como comportamento de ingestão). Ver "Comportamento de ingestão de regras do ILM" .

> Se sua grade incluir apenas um site, você não poderá usar o pool de armazenamento Todos os nós de armazenamento (StorageGRID 11.6 e anteriores) ou o site Todos os sites em um perfil de codificação de eliminação. Esse comportamento evita que o perfil se torne inválido se um segundo site for adicionado.

Habilitar proteção contra perda de site

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

A replicação e a codificação de eliminação exigem diferentes configurações de pool de armazenamento:

- Para usar a replicação para proteção contra perda de site, use os pools de armazenamento específicos do site que são criados automaticamente durante a instalação do StorageGRID . Em seguida, crie regras ILM com"instruções de posicionamento" que especificam vários pools de armazenamento para que uma cópia de cada objeto seja colocada em cada site.
- Para usar a codificação de eliminação para proteção contra perda de site,"criar pools de armazenamento que consistem em vários sites" . Em seguida, crie regras de ILM que usem um pool de armazenamento composto por vários sites e qualquer esquema de codificação de eliminação disponível.

> Ao configurar sua implantação do StorageGRID para proteção contra perda de site, você também deve levar em consideração os efeitos de"opções de ingestão" e"consistência" .

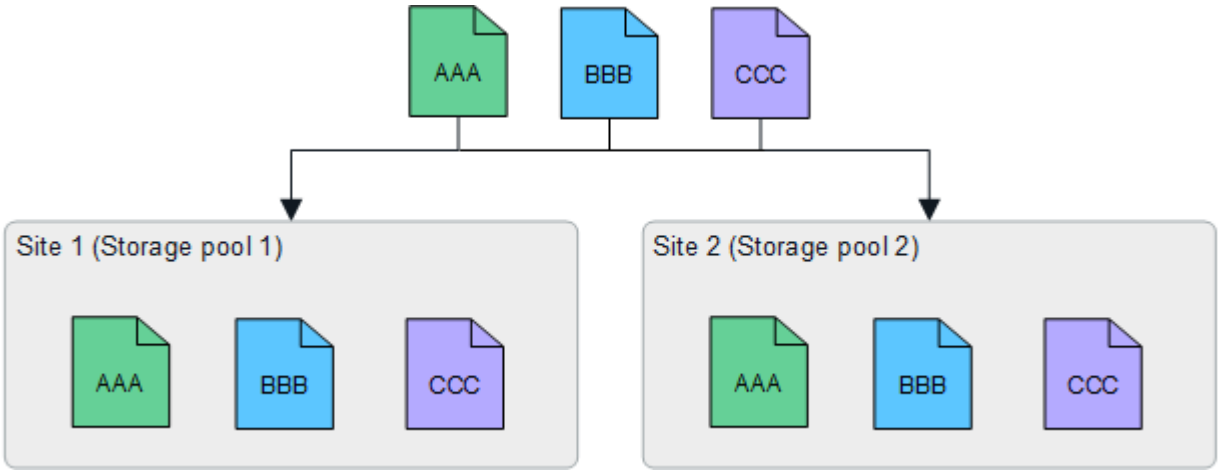
Exemplo de replicação

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

- O pool de armazenamento 1 contém o Site 1

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

Posicionamentos de regras do ILM:



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

Exemplo de codificação de apagamento

Ter pools de armazenamento que consistem em mais de um site por pool de armazenamento permite que você configure regras de ILM que usam codificação de eliminação para proteção contra perda de site. Neste exemplo:

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

Posicionamentos de regras do ILM:

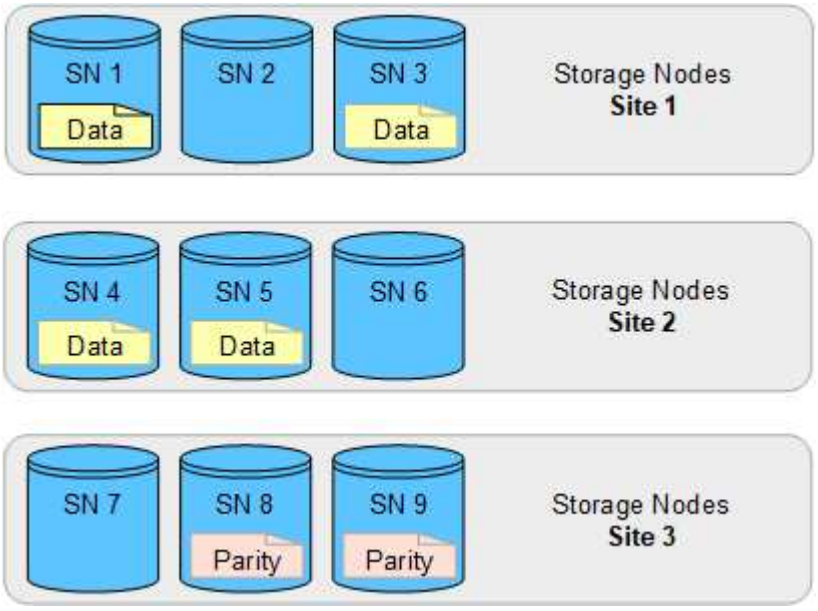
Neste exemplo:

- A regra ILM usa um esquema de codificação de apagamento 4+2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto.

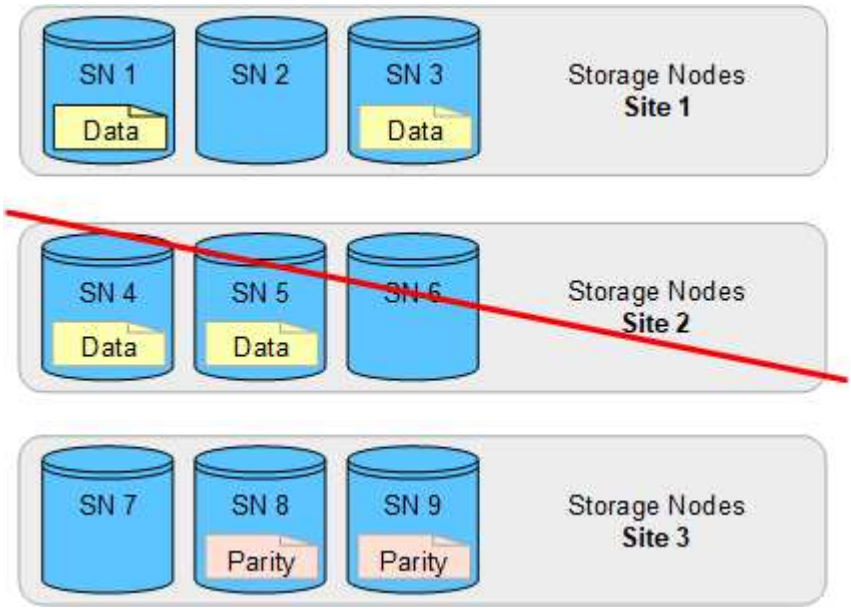
- Cada um dos seis fragmentos é armazenado em um nó diferente em três locais do data center para fornecer proteção de dados em caso de falhas de nó ou perda de local.

> A codificação de eliminação é permitida em pools de armazenamento que contêm qualquer número de sites *exceto* dois sites.

Regra ILM usando esquema de codificação de apagamento 4+2:



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



Criar um pool de armazenamento

Crie pools de armazenamento para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de armazenamento usado. Cada pool de armazenamento inclui um ou mais sites e um ou mais níveis de armazenamento.

> Quando você instala o StorageGRID 11.9 em uma nova grade, pools de armazenamento são criados automaticamente para cada site. No entanto, se você instalou inicialmente o StorageGRID 11.6 ou anterior, os pools de armazenamento não serão criados automaticamente para cada site.

Se você deseja criar pools de armazenamento em nuvem para armazenar dados de objetos fora do seu sistema StorageGRID , consulte o"informações sobre o uso de pools de armazenamento em nuvem" .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você revisou as diretrizes para criar pools de armazenamento.

Sobre esta tarefa

Os pools de armazenamento determinam onde os dados do objeto são armazenados. O número de pools de armazenamento necessários depende do número de sites na sua grade e dos tipos de cópias que você deseja: replicadas ou codificadas para eliminação.

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

> Não inclua o site Todos os sites em um pool de armazenamento que será usado em um perfil de codificação de eliminação. Em vez disso, adicione uma entrada separada ao pool de armazenamento para cada site que armazenará dados codificados para eliminação. Veresta etapa por exemplo.

- Se você tiver mais de um nível de armazenamento, não crie um pool de armazenamento que inclua diferentes níveis de armazenamento em um único local. Veja o"Diretrizes para criação de pools de armazenamento" .

Passos

1. Selecione **ILM** > **Pools de armazenamento**.

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

   > Para novas instalações do StorageGRID 11.6 ou anterior, o pool de armazenamento Todos os nós de armazenamento é atualizado automaticamente sempre que você adiciona novos sites de data center. Não use esse pool em regras de ILM.

2. Para criar um novo pool de armazenamento, selecione **Criar**.
3. Insira um nome exclusivo para o pool de armazenamento. Use um nome que seja fácil de identificar ao configurar perfis de codificação de eliminação e regras de ILM.
4. Na lista suspensa **Site**, selecione um site para este pool de armazenamento.

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

Em geral, não use o site Todos os Sites em nenhum pool de armazenamento. As regras do ILM que usam um pool de armazenamento Todos os Sites colocam objetos em qualquer site disponível, dando a você menos controle sobre o posicionamento dos objetos. Além disso, um pool de armazenamento de Todos os Sites usa os Nós de Armazenamento em um novo site imediatamente, o que pode não ser o comportamento esperado.

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

   O grau de armazenamento, *inclui todos os graus de armazenamento*, inclui todos os nós de armazenamento no local selecionado. Se você criou níveis de armazenamento adicionais para os Nós de Armazenamento na sua grade, eles serão listados no menu suspenso.

6. Se você quiser usar o pool de armazenamento em um perfil de codificação de eliminação de vários sites, selecione **Adicionar mais nós** para adicionar uma entrada para cada site ao pool de armazenamento.

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

   Para remover uma entrada, selecione o ícone de exclusão .

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

   O novo pool de armazenamento é adicionado à lista.

Ver detalhes do pool de armazenamento

Você pode visualizar os detalhes de um pool de armazenamento para determinar onde ele é usado e ver quais nós e níveis de armazenamento estão incluídos.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Passos

1. Selecione **ILM** > **Pools de armazenamento**.

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

   - **Nome**: O nome de exibição exclusivo do pool de armazenamento.
   - **Contagem de nós**: O número de nós no pool de armazenamento.
   - **Uso de armazenamento**: a porcentagem do espaço total utilizável que foi usada para dados de objeto neste nó. Este valor não inclui metadados do objeto.
   - **Capacidade total**: O tamanho do pool de armazenamento, que é igual à quantidade total de espaço utilizável para dados de objeto para todos os nós no pool de armazenamento.
   - **Uso do ILM**: como o pool de armazenamento está sendo usado atualmente. Um pool de armazenamento pode não estar sendo utilizado ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de eliminação ou ambos.

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

A página de detalhes do pool de armazenamento é exibida.

3. Veja a aba **Nós** para saber mais sobre os Nós de Armazenamento incluídos no pool de armazenamento.

   A tabela inclui as seguintes informações para cada nó:

   - Nome do nó
   - Nome do site
   - Grau de armazenamento
   - Uso de armazenamento: a porcentagem do espaço total utilizável para dados de objeto que foi usada para o nó de armazenamento.

   > O mesmo valor de uso de armazenamento (%) também é mostrado no gráfico Armazenamento usado - Dados do objeto para cada nó de armazenamento (selecione **NÓS** > ***Nó de armazenamento*** > **Armazenamento**).

4. Veja a aba **Uso do ILM** para determinar se o pool de armazenamento está sendo usado atualmente em alguma regra do ILM ou perfil de codificação de eliminação.
5. Opcionalmente, acesse a **página de regras do ILM** para saber mais e gerenciar quaisquer regras que usem o pool de armazenamento.

   Veja o"instruções para trabalhar com regras ILM" .

Editar pool de armazenamento

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você revisou o"diretrizes para criação de pools de armazenamento" .
- Se você planeja editar um pool de armazenamento usado por uma regra na política ILM ativa, você deve considerar como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

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

Passos

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

   Não é possível editar o pool de armazenamento Todos os nós de armazenamento (StorageGRID 11.6 e anteriores).

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

   Você não poderá alterar o site ou o nível de armazenamento se o pool de armazenamento for usado em um perfil de codificação de eliminação e a alteração fizer com que o esquema de codificação de eliminação se torne inválido. Por exemplo, se um pool de armazenamento usado em um perfil de codificação de eliminação atualmente inclui um nível de armazenamento com apenas um site, você não poderá usar um nível de armazenamento com dois sites porque a alteração tornaria o esquema de codificação de eliminação inválido.

   > Adicionar ou remover sites de um pool de armazenamento existente não moverá nenhum dado codificado para eliminação existente. Se quiser mover os dados existentes do site, você deverá criar um novo pool de armazenamento e um perfil EC para recodificar os dados.

6. Selecione **Salvar**.

Depois que você terminar

Se você adicionou um novo site ou nível de armazenamento a um pool de armazenamento usado na política de ILM ativa, ative uma nova política de ILM para forçar o StorageGRID a usar o novo site ou nível de armazenamento. Por exemplo, clone sua política de ILM existente e depois ative o clone. Ver "Trabalhar com regras e políticas do ILM" .

Remover um pool de armazenamento

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .

Passos

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

   Não é possível remover um pool de armazenamento se ele estiver sendo usado em uma regra de ILM ou em um perfil de codificação de eliminação. Conforme necessário, selecione ***nome do pool de armazenamento*** > **uso do ILM** para determinar onde o pool de armazenamento é usado.

3. Se o pool de armazenamento que você deseja remover não estiver sendo usado, marque a caixa de seleção.
4. Selecione **Remover**.
5. Selecione **OK**.

Use pools de armazenamento em nuvem

O que é um pool de armazenamento em nuvem?

Um pool de armazenamento em nuvem permite que você use o ILM para mover dados de objetos para fora do seu sistema StorageGRID . Por exemplo, você pode querer mover objetos acessados com pouca frequência para um armazenamento em nuvem de menor custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a camada de acesso Archive no armazenamento de Blobs do Microsoft Azure. Ou você pode querer manter um backup em nuvem dos objetos StorageGRID para melhorar a recuperação de desastres.

Da perspectiva do ILM, um pool de armazenamento em nuvem é semelhante a um pool de armazenamento. Para armazenar objetos em qualquer local, selecione o pool ao criar as instruções de posicionamento para uma regra ILM. No entanto, enquanto os pools de armazenamento consistem em nós de armazenamento dentro do sistema StorageGRID , um pool de armazenamento em nuvem consiste em um bucket externo (S3) ou contêiner (armazenamento de Blobs do Azure).

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

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

	Pool de armazenamento	Pool de armazenamento em nuvem
Onde os objetos são armazenados?	Em um ou mais nós de armazenamento dentro do StorageGRID.	Em um bucket do Amazon S3, contêiner de armazenamento de Blobs do Azure ou Google Cloud externo ao sistema StorageGRID . Se o Cloud Storage Pool for um bucket do Amazon S3: • Opcionalmente, você pode configurar um ciclo de vida de bucket para fazer a transição de objetos para armazenamento de baixo custo e longo prazo, como o Amazon S3 Glacier ou o S3 Glacier Deep Archive. O sistema de armazenamento externo deve oferecer suporte à classe de armazenamento Glacier e à API S3 RestoreObject. • Você pode criar pools de armazenamento em nuvem para uso com o AWS Commercial Cloud Services (C2S), que oferece suporte à AWS Secret Region. Se o Cloud Storage Pool for um contêiner de armazenamento de Blobs do Azure, o StorageGRID fará a transição do objeto para a camada de Arquivo. **Observação:** Em geral, não configure o gerenciamento do ciclo de vida do armazenamento de Blobs do Azure para o contêiner usado para um Pool de Armazenamento em Nuvem. As operações RestoreObject em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.
O que controla o posicionamento dos objetos?	Uma regra de ILM nas políticas de ILM ativas.	Uma regra de ILM nas políticas de ILM ativas.
Qual método de proteção de dados é usado?	Codificação de replicação ou eliminação.	Replicação.
Quantas cópias de cada objeto são permitidas?	Múltiplo.	Uma cópia no Cloud Storage Pool e, opcionalmente, uma ou mais cópias no StorageGRID. **Observação:** você não pode armazenar um objeto em mais de um pool de armazenamento em nuvem ao mesmo tempo.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo. **Observação**: os dados do FabricPool não podem ser hierarquizados em pools de armazenamento em nuvem.

Ciclo de vida de um objeto de pool de armazenamento em nuvem

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

S3: Ciclo de vida de um objeto de pool de armazenamento em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um pool de armazenamento em nuvem do S3.

> ⓘ "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 oferece suporte à camada de restauração Expedited. Somente a recuperação em massa ou padrão é suportada.

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

1. **Objeto armazenado no StorageGRID**

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

2. **Objeto movido para o S3 Cloud Storage Pool**
   - Quando o objeto é correspondido por uma regra do ILM que usa um S3 Cloud Storage Pool como seu local de posicionamento, o StorageGRID move o objeto para o bucket S3 externo especificado pelo Cloud Storage Pool.
   - Quando o objeto for movido para o S3 Cloud Storage Pool, o aplicativo cliente poderá recuperá-lo usando uma solicitação S3 GetObject do StorageGRID, a menos que o objeto tenha sido transferido para o armazenamento Glacier.
3. **Objeto transferido para Glacier (estado não recuperável)**
   - Opcionalmente, o objeto pode ser transferido para o armazenamento Glacier. Por exemplo, o bucket S3 externo pode usar a configuração do ciclo de vida para fazer a transição de um objeto para o armazenamento Glacier imediatamente ou após alguns dias.

     > ⓘ Se quiser fazer a transição de objetos, você deve criar uma configuração de ciclo de vida para o bucket S3 externo e usar uma solução de armazenamento que implemente a classe de armazenamento Glacier e suporte a API S3 RestoreObject.

   - Durante a transição, o aplicativo cliente pode usar uma solicitação S3 HeadObject para monitorar o status do objeto.
4. **Objeto restaurado do armazenamento Glacier**

   Se um objeto tiver sido transferido para o armazenamento Glacier, o aplicativo cliente poderá emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o S3 Cloud Storage Pool. A solicitação especifica por quantos dias a cópia deve ficar disponível no Cloud Storage Pool e o nível de acesso a dados a ser usado para a operação de restauração (Acelerado, Padrão ou em Massa). Quando a data de expiração da cópia recuperável for atingida, a cópia será automaticamente retornada ao estado não recuperável.

Se uma ou mais cópias do objeto também existirem em nós de armazenamento dentro do StorageGRID, não há necessidade de restaurar o objeto do Glacier emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. **Objeto recuperado**

   Depois que um objeto é restaurado, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Azure: Ciclo de vida de um objeto de pool de armazenamento em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto 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 pool de armazenamento em nuvem do Azure**

   Quando o objeto é correspondido por uma regra de ILM que usa um Pool de Armazenamento em Nuvem do Azure como seu local de posicionamento, o StorageGRID move o objeto para o contêiner de armazenamento de Blobs do Azure externo especificado pelo Pool de Armazenamento em Nuvem.

3. **Objeto transferido para o nível de arquivo (estado não recuperável)**

   Imediatamente após mover o objeto para o Pool de Armazenamento em Nuvem do Azure, o StorageGRID faz a transição automática do objeto para a camada de Arquivo de Armazenamento de Blobs do Azure.

4. **Objeto restaurado do nível de arquivo**

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

   Quando o StorageGRID recebe o RestoreObject, ele temporariamente faz a transição do objeto para a camada Cool do armazenamento de Blobs do Azure. Assim que a data de expiração na solicitação RestoreObject for atingida, o StorageGRID fará a transição do objeto de volta para a camada de arquivamento.

   Se uma ou mais cópias do objeto também existirem em nós de armazenamento dentro do StorageGRID, não haverá necessidade de restaurar o objeto da camada de acesso de arquivamento emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. **Objeto recuperado**

   Depois que um objeto for restaurado no Pool de Armazenamento em Nuvem do Azure, o aplicativo cliente poderá emitir uma solicitação GetObject para recuperar o objeto restaurado.

Informações relacionadas

"Usar API REST do S3"

Quando usar pools de armazenamento em nuvem

Usando pools de armazenamento em nuvem, você pode fazer backup ou hierarquizar dados em um local externo. Além disso, você pode fazer backup ou hierarquizar dados em mais de uma nuvem.

Faça backup dos dados do StorageGRID em um local externo

Você pode usar um Cloud Storage Pool para fazer backup de objetos do StorageGRID em um local externo.

Se as cópias no StorageGRID estiverem inacessíveis, os dados do objeto no Cloud Storage Pool poderão ser usados para atender às solicitações do cliente. No entanto, talvez seja necessário emitir uma solicitação S3 RestoreObject para acessar a cópia do objeto de backup no Cloud Storage Pool.

Os dados do objeto em um Cloud Storage Pool também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha no volume de armazenamento ou no nó de armazenamento. 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 armazenamento em nuvem.
2. Configure uma regra de ILM que armazene simultaneamente cópias de objetos em nós de armazenamento (como cópias replicadas ou codificadas para eliminação) e uma única cópia de objeto no pool de armazenamento em nuvem.
3. Adicione a regra à sua política de ILM. Em seguida, simule e ative a política.

Dados em camadas do StorageGRID para local externo

Você pode usar um Cloud Storage Pool para armazenar objetos fora do sistema StorageGRID . Por exemplo, suponha que você tenha um grande número de objetos que precisa manter, mas espera acessá-los raramente, ou nunca. Você pode usar um pool de armazenamento em nuvem para hierarquizar os objetos em armazenamentos de menor custo e liberar espaço no StorageGRID.

Para implementar uma solução em camadas:

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

Manter vários endpoints de nuvem

Você pode configurar vários pontos de extremidade do Cloud Storage Pool se quiser hierarquizar ou fazer backup de dados de objetos em mais de uma nuvem. Os filtros nas suas regras do ILM permitem que você especifique quais objetos são armazenados em cada pool do Cloud Storage. 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 de Blobs do Azure. Ou você pode querer mover dados entre o Amazon S3 Glacier e o armazenamento de Blobs do Azure.

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

Para implementar vários endpoints de nuvem:

1. Crie até 10 pools de armazenamento em nuvem.
2. Configure regras de 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 um determinado período e depois mova-os para o Cloud Storage Pool B.
3. Adicione as regras à sua política de ILM. Em seguida, simule e ative a política.

Considerações sobre pools de armazenamento em nuvem

Se você planeja usar um Cloud Storage Pool para mover objetos para fora do sistema StorageGRID , revise as considerações para configurar e usar Cloud Storage Pools.

Considerações gerais

- Em geral, o armazenamento de arquivo em nuvem, como o Amazon S3 Glacier ou o armazenamento de Blobs do Azure, é um local barato para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento de arquivos em nuvem são relativamente altos. Para atingir o menor custo geral, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um pool de armazenamento em nuvem é recomendado apenas para conteúdo que você espera acessar com pouca frequência.
- O uso de Cloud Storage Pools com FabricPool não é suportado devido à latência adicional para recuperar um objeto do destino do Cloud Storage Pool.
- Objetos com o S3 Object Lock ativado não podem ser colocados em pools de armazenamento em nuvem.
- Se o bucket S3 de destino para um pool de armazenamento em nuvem tiver o bloqueio de objeto S3 habilitado, a tentativa de configurar a replicação do bucket (PutBucketReplication) falhará com um erro AccessDenied.
- As seguintes combinações de plataforma, autenticação e protocolo com bloqueio de objeto S3 não são suportadas para pools de armazenamento em nuvem:
  - **Plataformas**: Google Cloud Platform e Azure
  - **Tipos de autenticação**: Funções do IAM em qualquer lugar e acesso anônimo
  - **Protocolo**: HTTP

Considerações sobre 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 seu 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, você também deve"configurar um proxy de armazenamento" para permitir que mensagens sejam enviadas para terminais externos, como um terminal na

Internet.

Considerações sobre custos

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

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

Custos mais significativos podem ser incorridos se você precisar mover objetos de um ponto de extremidade externo do Cloud Storage Pool 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 armazenamento em nuvem e você decide armazená-lo no StorageGRID . Nesse caso, você reconfigura suas regras e políticas de ILM. Quando ocorre a avaliação do ILM, o StorageGRID emite várias solicitações para recuperar o objeto do Cloud Storage Pool. O StorageGRID então cria o número especificado de cópias replicadas ou codificadas para eliminação localmente. Depois que o objeto é movido de volta para StorageGRID, a cópia no Cloud Storage Pool é excluída.
- Objetos são perdidos devido à falha do nó de armazenamento. 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 objetos são movidos de volta para o StorageGRID de um Cloud Storage Pool, o StorageGRID emite várias solicitações ao ponto de extremidade do Cloud Storage Pool para cada objeto. Antes de mover grandes quantidades 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

As políticas para o bucket S3 externo usado para um Cloud Storage Pool devem conceder permissão ao StorageGRID para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento Glacier quando necessário e muito mais. O ideal é que o StorageGRID tenha acesso de controle total ao bucket(`s3:*`); no entanto, se isso não for possível, a política de bucket deve conceder as seguintes permissões 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 bucket externo

A movimentação de objetos entre o StorageGRID e o bucket S3 externo especificado no Cloud Storage Pool é controlada pelas regras do ILM e pelas políticas ativas do ILM no StorageGRID. Em contraste, a transição de objetos do bucket S3 externo especificado no Cloud Storage Pool para o Amazon S3 Glacier ou S3 Glacier Deep Archive (ou para uma solução de armazenamento que implementa 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 RestoreObject do S3.

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

```
<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 eles foram criados (ou seja, no dia em que foram movidos do StorageGRID para o Cloud Storage Pool).

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

Se você deseja transferir objetos no Cloud Storage Pool para o S3 Glacier Deep Archive (em vez do 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 sobre a camada de acesso

Ao configurar uma conta de armazenamento do Azure, você pode definir o nível de acesso padrão como Quente ou Frio. Ao criar uma conta de armazenamento para uso com um pool de armazenamento em nuvem,

você deve usar o nível Hot como nível padrão. Embora o StorageGRID defina imediatamente o nível como Arquivar ao mover objetos para o Cloud Storage Pool, usar uma configuração padrão de Quente garante que você não será cobrado por uma taxa de exclusão antecipada para objetos removidos do nível Frio antes do mínimo de 30 dias.

Azure: Gerenciamento de ciclo de vida não suportado

Não use o gerenciamento do ciclo de vida do armazenamento de Blobs do Azure para o contêiner usado com um Pool de Armazenamento em Nuvem. As operações do ciclo de vida podem interferir nas operações do Cloud Storage Pool.

Informações relacionadas

"Criar um pool de armazenamento em nuvem"

Comparar pools de armazenamento em nuvem e replicação do CloudMirror

Ao começar a usar os Cloud Storage Pools, pode ser útil entender as semelhanças e diferenças entre os Cloud Storage Pools e o serviço de replicação StorageGRID CloudMirror.

	Pool de armazenamento em nuvem	Serviço de replicação CloudMirror
Qual é o objetivo principal?	Atua como um alvo de arquivo. A cópia do objeto no Cloud Storage Pool pode ser a única cópia do objeto ou pode ser uma cópia adicional. Ou seja, em vez de manter duas cópias no local, você pode manter uma cópia no StorageGRID e enviar uma cópia para o Cloud Storage Pool.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket S3 externo (destino). Cria uma cópia independente de um objeto em uma infraestrutura S3 independente.
Como é configurado?	Definido da mesma forma que os pools de armazenamento, usando o Grid Manager ou a Grid Management API. Pode ser selecionado como o local de posicionamento em uma regra ILM. Enquanto um pool de armazenamento consiste em um grupo de nós de armazenamento, um pool de armazenamento em nuvem é definido usando um ponto de extremidade remoto do S3 ou do Azure (endereço IP, credenciais e assim por diante).	Um usuário locatário"configura a replicação do CloudMirror" definindo um ponto de extremidade do CloudMirror (endereço IP, credenciais e assim por diante) usando o Tenant Manager ou a API do S3. Após a configuração do ponto de extremidade do CloudMirror, qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o ponto de extremidade do CloudMirror.
Quem é responsável por configurá-lo?	Normalmente, um administrador de rede	Normalmente, um usuário locatário

	Pool de armazenamento em nuvem	Serviço de replicação CloudMirror
Qual é o destino?	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Camada de arquivo de Blobs do Azure • Plataforma de nuvem do Google (GCP)	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3) • Plataforma de nuvem do Google (GCP)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras de ILM nas políticas de ILM ativas. As regras do ILM definem quais objetos o StorageGRID move para o Cloud Storage Pool e quando os objetos são movidos.	O ato de ingerir um novo objeto em um bucket de origem que foi configurado com um endpoint do CloudMirror. Objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são recuperados?	Os aplicativos devem fazer solicitações ao StorageGRID para recuperar objetos que foram movidos para um pool de armazenamento em nuvem. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivo, o StorageGRID gerencia o processo de restauração do objeto para que ele possa ser recuperado.	Como a cópia espelhada no bucket de destino é uma cópia independente, os aplicativos podem recuperar o objeto fazendo solicitações ao StorageGRID ou ao destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos para uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário usar o StorageGRID .
Você pode ler diretamente do destino?	Não. Os objetos movidos para um pool de armazenamento em nuvem são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação do Cloud Storage Pool).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da fonte?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído não existe mais no bucket StorageGRID , mas continua existindo no bucket de destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.
Como acessar objetos após um desastre (sistema StorageGRID não operacional)?	Nós 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 objetos no destino do CloudMirror são independentes do StorageGRID, portanto, podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Criar um pool de armazenamento em nuvem

Um pool de armazenamento em nuvem especifica um único bucket externo do Amazon S3 ou outro provedor compatível com S3 ou um contêiner de armazenamento de Blobs do Azure.

Ao criar um Pool de Armazenamento em Nuvem, você especifica o nome e o local do bucket ou contêiner externo que o StorageGRID usará para armazenar objetos, o tipo de provedor de nuvem (Amazon S3/GCP ou armazenamento de Blobs do Azure) e as informações que o StorageGRID precisa para acessar o bucket ou contêiner externo.

O StorageGRID valida o Cloud Storage Pool assim que você o salva, portanto, você deve garantir que o bucket ou contêiner especificado no Cloud Storage Pool exista e esteja acessível.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .
- Você revisou o"considerações para pools de armazenamento em nuvem" .
- O bucket ou contêiner externo referenciado pelo Cloud Storage Pool já existe e você tem oinformações do ponto de extremidade do serviço .
- Para acessar o balde ou contêiner, você tem oinformações da conta para o tipo de autenticação você escolherá.

Passos

1. Selecione **ILM** > **Pools de armazenamento** > **Pools de armazenamento em nuvem**.
2. Selecione **Criar** e insira as seguintes informações:

Campo	Descrição
Nome do pool de armazenamento em nuvem	Um nome que descreve brevemente o Cloud Storage Pool e sua finalidade. Use um nome que seja fácil de identificar ao configurar regras de ILM.
Tipo de provedor	Qual provedor de nuvem você usará para este pool de armazenamento em nuvem: • **Amazon S3/GCP**: Selecione esta opção para um Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou outro provedor compatível com S3. • **Armazenamento de Blobs do Azure**
Balde ou recipiente	O nome do bucket S3 externo ou do contêiner do Azure. Não é possível alterar esse valor depois que o Pool de Armazenamento em Nuvem for salvo.

3. Com base na seleção do tipo de provedor, insira as informações do ponto de extremidade do serviço.

Amazon S3/GCP

a. Para o protocolo, selecione HTTPS ou HTTP.

> Não use conexões HTTP para dados confidenciais.

b. Digite o nome do host. Exemplo:

`s3-aws-region.amazonaws.com`

c. Selecione o estilo de URL:

Opção	Descrição
Detecção automática	Tente detectar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, o StorageGRID usará um URL no estilo de caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Estilo de hospedagem virtual	Use uma URL de estilo de hospedagem virtual para acessar o bucket. URLs de estilo de hospedagem virtual incluem o nome do bucket como parte do nome de domínio. Exemplo: `https://bucket-name.s3.company.com/key-name`
Estilo de caminho	Use uma URL no estilo de caminho para acessar o bucket. URLs no estilo de caminho incluem o nome do bucket no final. Exemplo: `https://s3.company.com/bucket-name/key-name` **Observação:** A opção de URL no estilo de caminho não é recomendada e será descontinuada em uma versão futura do StorageGRID.

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

Armazenamento de Blobs do Azure

a. Usando um dos seguintes formatos, insira o URI para o ponto de extremidade do serviço.

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

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

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

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

Chave de acesso

Para Amazon S3/GCP ou outro provedor compatível com S3

a. **ID da chave de acesso**: insira o ID da chave de acesso para a conta que possui o bucket externo.
b. **Chave de acesso secreta**: Digite a chave de acesso secreta.

Funções IAM em qualquer lugar

Para o serviço AWS IAM Roles Anywhere

O StorageGRID usa o AWS Security Token Service (STS) para gerar dinamicamente um token de curta duração para acessar recursos da AWS.

a. **Região do AWS IAM Roles Anywhere**: selecione a região para o Cloud Storage Pool. Por exemplo, `us-east-1` .
b. **URN da âncora de confiança**: insira o URN da âncora de confiança que valida solicitações de credenciais STS de curta duração. Pode ser uma CA raiz ou intermediária.
c. **URN do perfil**: insira o URN do perfil do IAM Roles Anywhere que lista as funções que podem ser assumidas por qualquer pessoa confiável.
d. **URN da função**: insira o URN da função do IAM que pode ser assumido por qualquer pessoa confiável.
e. **Duração da sessão**: insira a duração das credenciais de segurança temporárias e da sessão de função. Insira pelo menos 15 minutos e não mais que 12 horas.
f. **Certificado de CA do servidor** (opcional): Um ou mais certificados de CA confiáveis, no formato PEM, para verificar o servidor do IAM Roles Anywhere. Se omitido, o servidor não será verificado.
g. **Certificado de entidade final**: A chave pública, no formato PEM, do certificado X509 assinado pela âncora de confiança. O AWS IAM Roles Anywhere usa essa chave para emitir um token STS.
h. **Chave privada da entidade final**: A chave privada para o certificado da entidade final.

CAP (portal de acesso C2S)

Para serviços de nuvem comercial (C2S) serviço S3

a. **URL de credenciais temporárias**: insira a URL completa que o StorageGRID usará para obter credenciais temporárias do servidor CAP, incluindo todos os parâmetros de API obrigatórios e opcionais atribuídos à sua conta C2S.
b. **Certificado CA do servidor**: Selecione **Procurar** e carregue o certificado CA que o StorageGRID usará para verificar o servidor CAP. O certificado deve ser codificado em PEM e emitido por uma Autoridade Certificadora (CA) governamental apropriada.
c. **Certificado do cliente**: Selecione **Procurar** e carregue o certificado que o StorageGRID usará para se identificar no servidor CAP. O certificado do cliente deve ser codificado em PEM, emitido por uma Autoridade de Certificação Governamental (CA) apropriada e ter acesso concedido à sua conta C2S.
d. **Chave privada do cliente**: Selecione **Procurar** e carregue a chave privada codificada em PEM para o certificado do cliente.
e. Se a chave privada do cliente estiver criptografada, insira a senha para descriptografá-la. Caso contrário, deixe o campo **Senha da chave privada do cliente** em branco.

Se o certificado do cliente for criptografado, use o formato tradicional para a criptografia. O formato criptografado PKCS #8 não é suportado.

Armazenamento de Blobs do Azure

Para Armazenamento de Blobs do Azure, somente Chave Compartilhada

a. **Nome da conta**: Insira o nome da conta de armazenamento que possui o contêiner externo
b. **Chave da conta**: Insira a chave secreta da conta de armazenamento

Você pode usar o portal do Azure para encontrar esses valores.

Anônimo

Nenhuma informação adicional é necessária.

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

Opção	Descrição
Usar certificados de CA raiz no sistema operacional do nó de armazenamento	Use os certificados Grid CA instalados no sistema operacional para proteger conexões.
Usar certificado CA personalizado	Use um certificado CA personalizado. Selecione **Procurar** e carregue o certificado codificado em PEM.
Não verificar certificado	Selecionar esta opção significa que as conexões TLS com o Cloud Storage Pool não são seguras.

6. Selecione **Salvar**.

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

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

     Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro explicando o motivo da falha. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o bucket ou contêiner especificado ainda não existir.

7. Se ocorrer um erro, consulte o"instruções para solução de problemas de pools de armazenamento em nuvem" , resolva quaisquer problemas e tente salvar o Cloud Storage Pool novamente.

Ver detalhes do pool de armazenamento em nuvem

Você pode visualizar os detalhes de um pool de armazenamento em nuvem para determinar onde ele é usado e ver quais nós e níveis de armazenamento estão incluídos.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Passos

1. Selecione **ILM** > **Pools de armazenamento** > **Pools de armazenamento em nuvem**.

   A tabela Pools de armazenamento em nuvem inclui as seguintes informações para cada pool de armazenamento em nuvem que inclui nós de armazenamento:

   - **Nome**: O nome de exibição exclusivo do pool.
   - **URI**: O Identificador Uniforme de Recursos do Pool de Armazenamento em Nuvem.
   - **Tipo de provedor**: Qual provedor de nuvem é usado para este pool de armazenamento em nuvem.
   - **Container**: O nome do bucket usado para o Cloud Storage Pool.
   - **Uso do ILM**: Como o pool está sendo usado atualmente. Um pool de armazenamento em nuvem pode não estar sendo utilizado ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de eliminação ou ambos.
   - **Último erro**: O último erro detectado durante uma verificação de integridade deste pool de armazenamento em nuvem.
2. Para visualizar detalhes de um pool de armazenamento em nuvem específico, selecione seu nome.

   A página de detalhes do pool é exibida.
3. Veja a aba **Autenticação** para saber mais sobre o tipo de autenticação para este Pool de Armazenamento em Nuvem e para editar os detalhes de autenticação.
4. Veja a aba **Verificação do servidor** para saber mais sobre detalhes da verificação, editar a verificação, baixar um novo certificado ou copiar o PEM do certificado.
5. Veja a aba **Uso do ILM** para determinar se o Cloud Storage Pool está sendo usado atualmente em alguma regra do ILM ou perfil de codificação de eliminação.
6. Opcionalmente, vá para a **página de regras do ILM** para"aprender e gerenciar quaisquer regras" que usam o Cloud Storage Pool.

Editar 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 S3 ou o contêiner do Azure para um Pool de Armazenamento em Nuvem.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você revisou o"considerações para pools de armazenamento em nuvem" .

Passos

1. Selecione **ILM** > **Pools de armazenamento** > **Pools de armazenamento em nuvem**.

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

2. Marque a caixa de seleção do Pool de Armazenamento em Nuvem que você deseja editar e selecione **Ações** > **Editar**.

   Como alternativa, selecione o nome do Pool de Armazenamento em Nuvem e selecione **Editar**.

3. Conforme necessário, altere o nome do pool de armazenamento em nuvem, o ponto de extremidade do serviço, as credenciais de autenticação ou o método de verificação do certificado.

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

   Se você já carregou um certificado de servidor ou cliente, pode expandir o acordeão **Detalhes do certificado** para revisar o certificado que está em uso no momento.

4. Selecione **Salvar**.

   Quando você salva um pool de armazenamento em nuvem, o StorageGRID valida se o bucket ou contêiner e o ponto de extremidade de serviço existem e se podem ser acessados 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.

   Veja as instruções para"solução de problemas de pools de armazenamento em nuvem" , resolva o problema e tente salvar o Cloud Storage Pool novamente.

Remover um pool de armazenamento em nuvem

Você pode remover um pool de armazenamento em nuvem se ele não for usado em uma regra de ILM e não contiver dados de objeto.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .

Se necessário, use o ILM para mover dados do objeto

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

Passos

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

   Não é possível remover um pool de armazenamento em nuvem se ele estiver sendo usado em uma regra de ILM ou em um perfil de codificação de eliminação.

3. Se o Cloud Storage Pool estiver sendo usado, selecione ***nome do pool de armazenamento em nuvem*** > **uso do ILM**.
4. "Clonar cada regra ILM"que atualmente coloca objetos no Cloud Storage Pool que você deseja remover.

5. Determine para onde você deseja mover os objetos existentes gerenciados por cada regra clonada.

   Você pode usar um ou mais pools de armazenamento ou um pool de armazenamento em nuvem diferente.

6. Edite cada uma das regras que você clonou.

   Para a Etapa 2 do assistente Criar regra ILM, selecione o novo local no campo **cópias em**.

7. "Criar uma nova política de ILM"e substituir cada uma das regras antigas por uma regra clonada.
8. Ative a nova política.
9. Aguarde o ILM remover objetos do Cloud Storage Pool e colocá-los no novo local.

Excluir pool de armazenamento em nuvem

Quando o Cloud Storage Pool estiver vazio e não for usado em nenhuma regra do ILM, você poderá excluí-lo.

Antes de começar

- Você removeu todas as regras do ILM que poderiam ter usado o pool.
- Você confirmou que o bucket S3 ou o contêiner do Azure não contém nenhum objeto.

  Ocorrerá um erro se você tentar remover um pool de armazenamento em nuvem se ele contiver objetos. Ver "Solucionar problemas de pools de armazenamento em nuvem" .

> Quando você cria um Cloud Storage Pool, o StorageGRID grava um arquivo marcador no bucket ou contêiner para identificá-lo como um Cloud Storage Pool. Não remova este arquivo, que é chamado `x-ntap-sgws-cloud-pool-uuid` .

Passos

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

Solucionar problemas de pools de armazenamento em nuvem

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

Determinar se ocorreu um erro

O StorageGRID executa uma verificação de integridade simples em cada pool de armazenamento em nuvem lendo o objeto conhecido `x-ntap-sgws-cloud-pool-uuid` para garantir que o Cloud Storage Pool possa ser acessado e esteja funcionando corretamente. Quando o StorageGRID encontra um erro no endpoint, ele executa uma verificação de integridade a cada minuto em cada nó de armazenamento. Quando o erro for resolvido, as verificações de integridade serão interrompidas. Se uma verificação de integridade detectar um problema, uma mensagem será exibida na coluna Último erro da tabela Pools de armazenamento em nuvem na página Pools de armazenamento.

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

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

Verifique se um erro foi resolvido

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

Se o problema subjacente tiver sido resolvido, a mensagem de erro não será mais exibida. Entretanto, se o problema subjacente não tiver sido corrigido (ou se um erro diferente for encontrado), a mensagem de erro será exibida na coluna Último erro dentro de alguns minutos.

Erro: Falha na verificação de integridade. Erro do ponto final

Você pode encontrar esse erro ao habilitar o S3 Object Lock com retenção padrão para seu bucket do Amazon S3 depois de começar a usar esse bucket para um Cloud Storage Pool. Este erro ocorre quando a operação PUT não tem um cabeçalho HTTP com um valor de soma de verificação de carga útil, como `Content-MD5` . Este valor de cabeçalho é exigido pela AWS para operações PUT em buckets com o S3 Object Lock habilitado.

Para corrigir esse problema, siga as etapas em"Editar um pool de armazenamento em nuvem" sem fazer nenhuma alteração. Esta ação aciona a validação da configuração do Cloud Storage Pool que detecta e atualiza automaticamente o sinalizador de bloqueio de objeto do S3 em uma configuração de ponto de extremidade do Cloud Storage Pool.

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 bucket ou contêiner incluir o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador, mas esse arquivo não tem o campo de metadados com o UUID esperado.

Normalmente, você só verá esse erro se estiver criando um novo Cloud Storage Pool e outra instância do StorageGRID já estiver usando o mesmo Cloud Storage Pool.

Tente uma destas etapas para corrigir o problema:

- Se você estiver configurando um novo pool de armazenamento em nuvem e o bucket contiver o `x-ntap-sgws-cloud-pool-uuid` arquivo e chaves de objeto adicionais semelhantes ao exemplo a seguir, crie um novo bucket e use esse novo bucket.

  Exemplo de uma chave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Se o `x-ntap-sgws-cloud-pool-uuid` o arquivo é o único objeto no bucket, exclua este arquivo.

Se essas etapas não se aplicarem ao seu cenário, entre em contato com o suporte.

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

Você pode encontrar esse erro nas seguintes circunstâncias:

- Quando você tenta criar ou editar um pool de armazenamento em nuvem.
- Quando você seleciona uma plataforma, autenticação ou combinação de protocolo não suportada com o S3 Object Lock durante a configuração de um novo Cloud Storage Pool. Ver "Considerações sobre pools de armazenamento em nuvem" .

Este erro indica que um problema de conectividade ou configuração está impedindo o StorageGRID de gravar no Cloud Storage Pool.

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

- Se a mensagem de erro contiver `Get *url*: EOF` , verifique se o ponto de extremidade de serviço usado para o Cloud Storage Pool não usa HTTP para um contêiner 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 ponto de extremidade de serviço usado para o pool de armazenamento em nuvem.
- Se o erro for devido a uma plataforma, autenticação ou protocolo não suportado, altere para uma configuração suportada com o S3 Object Lock e tente salvar o novo Cloud Storage Pool novamente.
- Para todas as outras mensagens de erro de endpoint, tente uma ou mais das seguintes opções:
  - Crie um contêiner 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 contêiner ou bucket especificado para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool 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 inserido ao configurar o Cloud Storage Pool.

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

Erro: Um pool de armazenamento em nuvem com este 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 qualquer um dos seguintes:

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

Tente uma ou mais destas etapas 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 ponto final

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

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

Erro: Objetos já foram colocados neste bucket

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 que foram movidos para lá pelo ILM, dados que estavam no bucket antes de você configurar o pool de armazenamento em nuvem ou dados que foram colocados no bucket por alguma outra fonte depois que o pool de armazenamento em nuvem foi criado.

Tente uma ou mais destas etapas para corrigir o problema:

- Siga as instruções para mover objetos de volta para o StorageGRID em "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 posteriormente um objeto excluído manualmente do StorageGRID, o objeto excluído não será encontrado.

Erro: O proxy encontrou um erro externo ao tentar acessar o Cloud Storage Pool

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

Tente uma ou mais destas etapas para corrigir o problema:

- Verifique as configurações do Cloud Storage Pool (**ILM** > **Storage pools**).
- Verifique a configuração de rede do servidor proxy de armazenamento.

Erro: O certificado X.509 está fora do período de validade

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Este erro ocorre quando a autenticação requer um certificado X.509 para garantir que o pool de armazenamento em nuvem externo correto seja validado e que o pool externo esteja vazio antes que a configuração do pool de armazenamento em nuvem seja excluída.

Tente estas etapas para corrigir o problema:

- Atualize o certificado configurado para autenticação no Cloud Storage Pool.
- Certifique-se de que qualquer alerta de expiração de certificado neste pool de armazenamento em nuvem seja resolvido.

Informações relacionadas

"Ciclo de vida de um objeto de pool de armazenamento em nuvem"

Gerenciar perfis de codificação de eliminação

Você pode visualizar os detalhes de um perfil de codificação de eliminação e renomear um perfil, se necessário. Você pode desativar um perfil de codificação de eliminação se ele não estiver sendo usado atualmente em nenhuma regra do ILM.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .

Ver detalhes do perfil de codificação de eliminação

Você pode visualizar os detalhes de um perfil de codificação de eliminação para determinar seu status, o esquema de codificação de eliminação usado e outras informações.

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Codificação de eliminação**.
2. Selecione o perfil. A página de detalhes do perfil é exibida.
3. Opcionalmente, visualize a guia Regras do ILM para obter uma lista de regras do ILM que usam o perfil e as políticas do ILM que usam essas regras.
4. Opcionalmente, visualize a guia Nós de Armazenamento para obter detalhes sobre cada Nó de Armazenamento no pool de armazenamento do perfil, como o local onde ele está localizado e o uso do armazenamento.

Renomear um perfil de codificação de eliminação

Talvez você queira renomear um perfil de codificação de eliminação para deixar mais óbvio o que o perfil faz.

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Codificação de eliminação**.
2. Selecione o perfil que você deseja renomear.
3. Selecione **Renomear**.
4. Insira um nome exclusivo para o perfil de codificação de eliminação.

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

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

5. Selecione **Salvar**.

Desativar um perfil de codificação de eliminação

Você pode desativar um perfil de codificação de eliminação se não planeja mais usá-lo e se o perfil não estiver

sendo usado atualmente em nenhuma regra do ILM.

> Confirme se não há operações de reparo de dados codificados para eliminação ou procedimentos de desativação em andamento. Uma mensagem de erro será retornada se você tentar desativar um perfil de codificação de eliminação enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

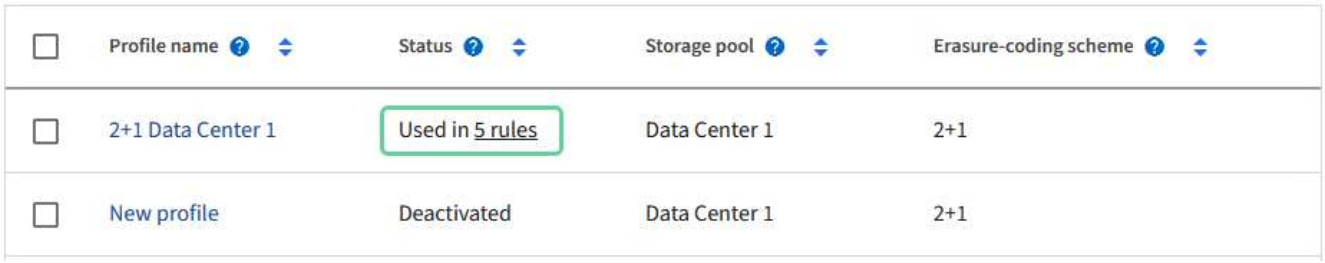
O StorageGRID impede que você desative um perfil de codificação de eliminação se qualquer uma das seguintes condições for verdadeira:

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Codificação de eliminação**.
2. Na guia Ativo, revise a coluna **Status** para confirmar se o perfil de codificação de eliminação que você deseja desativar não é usado em nenhuma regra do ILM.

   Não é possível desativar um perfil de codificação de eliminação se ele for usado em qualquer regra do ILM. No exemplo, o perfil 2+1 Data Center 1 é usado em pelo menos uma regra ILM.



3. Se o perfil for usado em uma regra ILM, siga estas etapas:
   a. Selecione **ILM** > **Regras**.
   b. Selecione cada regra e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de eliminação que você deseja desativar.
   c. Se a regra do ILM usar o perfil de codificação de eliminação que você deseja desativar, determine se a regra é usada em alguma política do ILM.
   d. Conclua as etapas adicionais na tabela, com base em onde o perfil de codificação de eliminação 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 necessárias etapas adicionais. Continue com este procedimento.	*Nenhum*

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que nunca foi usada em nenhuma política ILM	i. Edite ou exclua todas as regras de ILM afetadas. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de eliminação. ii. Continue com este procedimento.	"Trabalhar com regras e políticas do ILM"
Em uma regra de ILM que está atualmente em uma política de ILM ativa	i. Clone a política. ii. Remova a regra ILM que usa o perfil de codificação de eliminação. iii. Adicione uma ou mais novas regras de ILM para garantir que os objetos estejam protegidos. iv. Salve, simule e ative a nova política. v. Aguarde a aplicação da nova política e a movimentação dos objetos existentes 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 eliminação enquanto ele ainda estiver associado aos dados, a operação de desativação falhará. Uma mensagem de erro informará se o perfil ainda não estiver pronto para ser desativado. vi. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de eliminação. vii. Continue com este procedimento.	"Criar uma política de ILM" "Trabalhar com regras e políticas do ILM"

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra de ILM que está atualmente em uma política de ILM	i. Edite a política. ii. Remova a regra ILM que usa o perfil de codificação de eliminação. iii. Adicione uma ou mais novas regras de ILM para garantir que todos os objetos estejam protegidos. iv. Salve a política. v. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de eliminação. vi. Continue com este procedimento.	"Criar uma política de ILM" "Trabalhar com regras e políticas do ILM"

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

4. Se o perfil não for usado em uma regra ILM, selecione o botão de opção e selecione **Desativar**. A caixa de diálogo Desativar perfil de codificação de eliminação é exibida.

> Você pode selecionar vários perfis para desativar ao mesmo tempo, desde que cada perfil não seja usado em nenhuma regra.

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

Resultados

- Se o StorageGRID conseguir desativar o perfil de codificação de eliminação, seu status será Desativado. Você não pode mais selecionar este perfil para nenhuma regra do ILM. Você não pode reativar um perfil desativado.
- Se o StorageGRID não conseguir desativar o perfil, uma mensagem de erro será exibida. Por exemplo, uma mensagem de erro aparece se os dados do objeto ainda estiverem associados a este perfil. Pode ser necessário esperar várias semanas antes de tentar o processo de desativação novamente.

Configurar regiões (opcional e somente S3)

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

Se você quiser usar uma região de bucket do S3 como um filtro em uma regra, primeiro crie as regiões que podem ser usadas pelos buckets no seu sistema.

> Não é possível alterar a região de um bucket depois que ele foi criado.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

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

Ao criar uma regra de ILM, você pode querer usar a região associada a um bucket do S3 como um filtro avançado. Por exemplo, você pode criar uma regra que se aplique somente a objetos em buckets S3 criados no `us-west-2` região. Você pode então especificar que cópias desses objetos sejam colocadas em nós de armazenamento em um site de data center dentro dessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os buckets são considerados pertencentes ao `us-east-1` região.
- Você deve criar as regiões usando o Grid Manager antes de poder especificar uma região não padrão ao criar buckets usando o Tenant Manager ou a Tenant Management API ou com o elemento de solicitação LocationConstraint para solicitações da S3 PUT Bucket API. Ocorrerá um erro se uma solicitação PUT Bucket usar uma região que não foi definida em StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket S3. Os nomes de regiões diferenciam maiúsculas de minúsculas. Caracteres válidos são números, letras e hifens.

  > UE não é considerado um alias para eu-west-1. Se você quiser usar a região UE ou eu-west-1, deverá usar o nome exato.

- Você não pode excluir ou modificar uma região se ela for usada em uma regra atribuída a qualquer política (ativa ou inativa).
- Se você usar uma região inválida como filtro avançado em uma regra de ILM, não poderá adicionar essa regra a uma política.

  Uma região inválida pode ocorrer se você usar uma região como um filtro avançado em uma regra ILM, mas depois excluir essa região, ou se usar a API de gerenciamento de grade para criar uma regra e especificar uma região que você não definiu.

- Se você excluir uma região após usá-la para criar um bucket do S3, será necessário adicioná-la novamente se quiser usar o filtro avançado Restrição de Localização para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM** > **Regiões**.

   A página Regiões é exibida, com as regiões definidas atualmente listadas. **Região 1** mostra a região padrão, `us-east-1` , que não pode ser modificado ou removido.

2. Para adicionar uma região:
   a. Selecione **Adicionar outra região**.
   b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

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

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

   Uma mensagem de erro aparece se você tentar remover uma região que está sendo usada atualmente em qualquer política (ativa ou inativa).

4. Quando terminar de fazer as alterações, selecione **Salvar**.

   Agora você pode selecionar essas regiões na seção Filtros avançados na etapa 1 do assistente Criar regra ILM. Ver "Usar filtros avançados em regras de ILM" .

Criar regra ILM

Use regras do ILM para gerenciar objetos

Para gerenciar objetos, crie um conjunto de regras de gerenciamento do ciclo de vida das informações (ILM) e organize-as em uma política de 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.

> ⓘ Metadados de objetos não são gerenciados por regras de ILM. Em vez disso, os metadados do objeto são armazenados em um banco de dados Cassandra no que é conhecido como repositório de metadados. Três cópias dos metadados do objeto são mantidas automaticamente em cada site para proteger os dados contra perdas.

Elementos de uma regra ILM

Uma regra ILM tem três elementos:

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

Filtragem de regras ILM

Ao criar uma regra de ILM, você especifica filtros para identificar a 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 de ILM. A regra padrão fornece instruções de armazenamento para objetos que não correspondem aos filtros de outra regra.

- Filtros básicos permitem que você aplique regras diferentes a grupos grandes e distintos de objetos.

Esses filtros permitem que você aplique uma regra a contas de locatários específicas, buckets S3 específicos ou ambos.

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 a requisitos regulatórios, enquanto os dados do departamento de marketing podem precisar ser armazenados para facilitar as operações diárias. Depois de criar contas de locatários separadas para cada departamento ou depois de segregar dados dos diferentes departamentos em buckets S3 separados, você pode facilmente criar uma regra que se aplica a todos os registros financeiros e uma segunda regra que se aplica a todos os dados de marketing.

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

Você pode filtrar objetos com base em critérios muito específicos. Por exemplo, objetos armazenados pelo departamento de imagem de um hospital podem ser usados com frequência quando têm menos de 30 dias e com pouca frequência depois disso, enquanto objetos que contêm informações de visitas de pacientes podem precisar ser copiados para o departamento de cobrança na sede da rede de saúde. Você pode criar filtros que identifiquem cada tipo de objeto com base no nome do objeto, tamanho, tags de objeto S3 ou qualquer outro critério relevante e, em seguida, criar regras separadas para armazenar cada conjunto de objetos adequadamente.

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

Instruções de posicionamento de regras 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 posicionamento. Cada instrução de colocação se aplica a um único período de tempo.

Ao criar instruções de posicionamento:

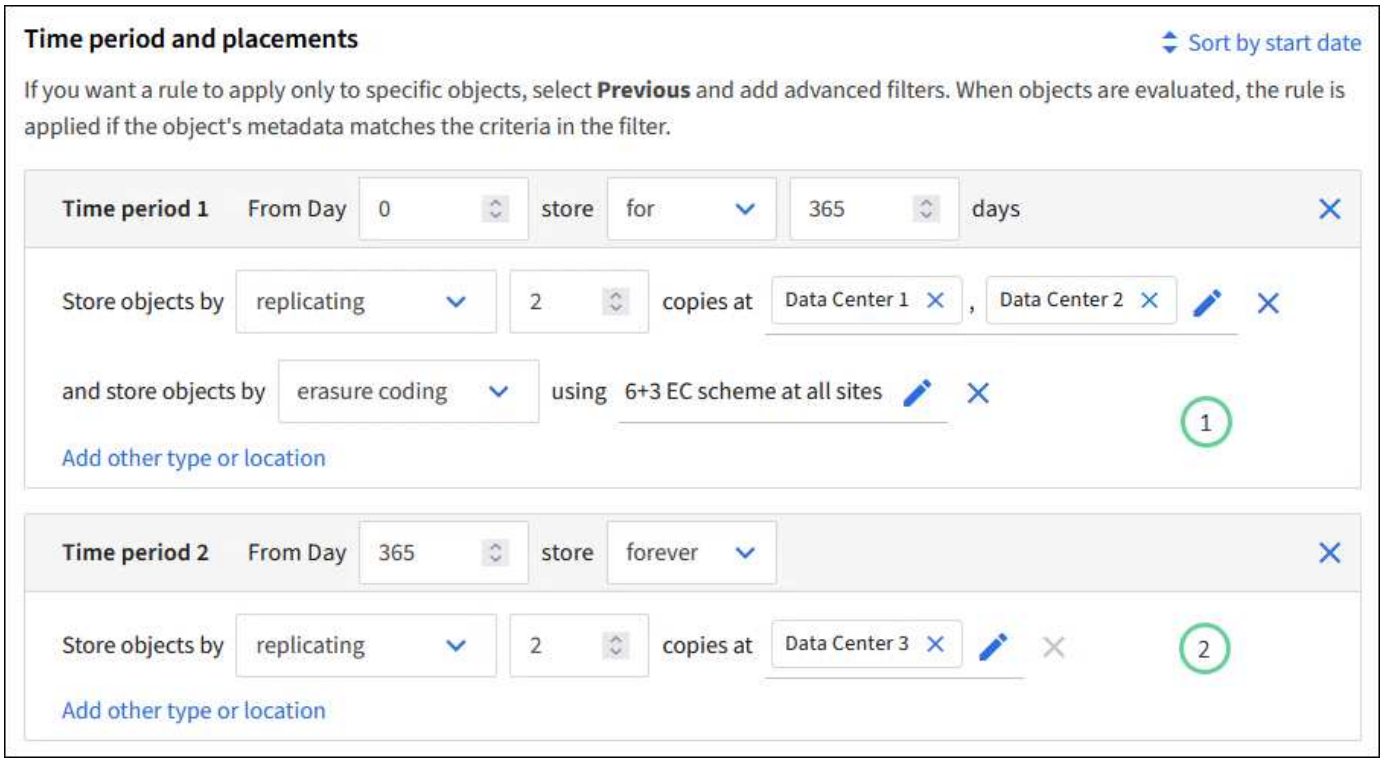
- Comece especificando o tempo de referência, que determina quando as instruções de posicionamento começam. O tempo de referência pode ser quando um objeto é ingerido, quando um objeto é acessado, quando um objeto versionado se torna inativo ou um tempo definido pelo usuário.
- Em seguida, você especifica quando o posicionamento será aplicado, em relação ao tempo de referência. Por exemplo, um posicionamento pode começar no dia 0 e continuar por 365 dias, em relação a quando o objeto foi ingerido.

- Por fim, você especifica o tipo de cópias (replicação ou codificação de eliminação) e o local onde as cópias são armazenadas. Por exemplo, você pode querer armazenar duas cópias replicadas em dois locais diferentes.

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

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

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



A primeira instrução de posicionamento (1) tem duas linhas para o primeiro ano:

- A primeira linha cria duas cópias de objetos replicados em dois sites de data center.
- A segunda linha cria uma cópia codificada para eliminação 6+3 usando todos os sites do data center.

A segunda instrução de posicionamento (2) cria duas cópias após um ano e as mantém para sempre.

Ao definir o conjunto de instruções de posicionamento para uma regra, você deve garantir que pelo menos uma instrução de posicionamento comece no dia 0, que não haja intervalos entre os períodos de tempo definidos e que a instrução de posicionamento final continue para sempre ou até que você não precise mais de cópias de objetos.

À medida que cada período da regra expira, as instruções de posicionamento de conteúdo para o próximo período são aplicadas. Novas cópias de objetos são criadas e quaisquer cópias desnecessárias são

excluídas.

Comportamento de ingestão de regras do ILM

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

- **Balanceado**: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM na ingestão; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.
- **Rigoroso**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.
- **Dual commit**: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Informações relacionadas

- "Opções de ingestão"
- "Vantagens, desvantagens e limitações das opções de ingestão"
- "Como a consistência e as regras do ILM interagem para afetar a proteção de dados"

Exemplo de regra ILM

Por exemplo, uma regra ILM poderia especificar o seguinte:

- Aplicar somente aos objetos pertencentes ao Locatário A.
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um local diferente.
- Mantenha as duas cópias "para sempre", o que significa que o StorageGRID não as excluirá automaticamente. Em vez disso, o StorageGRID manterá esses objetos até que eles sejam excluídos por uma solicitação de exclusão do cliente ou pelo término do ciclo de vida de um bucket.
- Use a opção Balanceado para o comportamento de ingestão: a instrução de posicionamento de dois sites é aplicada assim que o Locatário A salva um objeto no StorageGRID, a menos que não seja possível fazer imediatamente as duas cópias necessárias.

  Por exemplo, se o Site 2 estiver inacessível quando o Locatário A salvar um objeto, o StorageGRID fará duas cópias provisórias nos Nós de Armazenamento no Site 1. Assim que o Site 2 estiver disponível, o StorageGRID fará a cópia necessária naquele site.

Informações relacionadas

- "O que é um pool de armazenamento"
- "O que é um pool de armazenamento em nuvem"

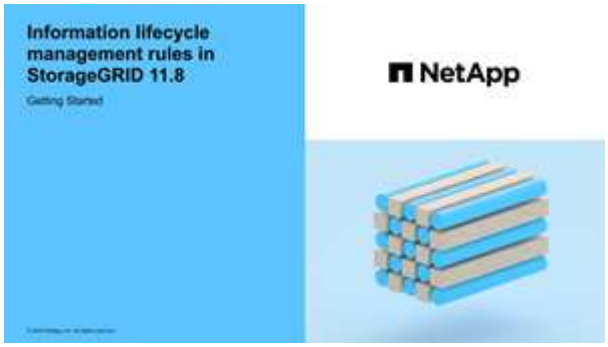
Acesse o assistente Criar uma regra ILM

As regras do ILM permitem que você gerencie o posicionamento dos dados do objeto ao longo do tempo. Para criar uma regra de ILM, use o assistente Criar uma regra de ILM.

> Se você quiser criar a regra ILM padrão para uma política, siga o"instruções para criar uma regra ILM padrão" em vez de.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Se você quiser especificar a quais contas de locatários esta regra se aplica, você tem o"Permissão de contas de inquilino" ou você sabe o ID da conta de cada conta.
- Se você quiser que a regra filtre objetos com base nos metadados do último horário de acesso, as atualizações do último horário de acesso devem ser habilitadas pelo bucket do S3.
- Você configurou todos os pools de armazenamento em nuvem que planeja usar. Ver "Criar pool de armazenamento em nuvem" .
- Você está familiarizado com o"opções de ingestão" .
- Se você precisar criar uma regra compatível para uso com o S3 Object Lock, você está familiarizado com o"requisitos para bloqueio de objeto S3" .
- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral das regras do ILM" .



Sobre esta tarefa

Ao criar regras de ILM:

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

Passos

1. Selecione **ILM** > **Regras**.
2. Selecione **Criar**. "Etapa 1 (Insira os detalhes)"do assistente Criar uma regra ILM é exibido.

Etapa 1 de 3: Insira os detalhes

A etapa **Inserir detalhes** do assistente Criar uma regra ILM permite que você insira um nome e uma descrição para a regra e defina filtros para a regra.

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

Sobre esta tarefa

Ao avaliar um objeto em relação a um"Regra ILM" O StorageGRID compara os metadados do objeto com os filtros da regra. Se os metadados do objeto corresponderem a todos os filtros, o StorageGRID usará a regra para posicionar o objeto. Você pode criar uma regra para aplicar a todos os objetos ou especificar filtros básicos, como uma ou mais contas de locatários ou nomes de buckets, ou filtros avançados, como o tamanho do objeto ou metadados do usuário.

Passos

1. Digite um nome exclusivo para a regra no campo **Nome**.
2. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.

   Você deve descrever o propósito ou a função da regra para poder reconhecê-la mais tarde.

3. Opcionalmente, selecione uma ou mais contas de locatário do S3 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 de contas de locatário, não poderá selecionar locatários da lista. Em vez disso, insira o ID do locatário ou insira vários IDs como uma sequência de caracteres delimitada por vírgulas.

4. Opcionalmente, especifique os buckets do S3 aos quais esta regra se aplica.

   Se **aplica-se a todos os buckets** for selecionado (padrão), a regra será aplicada a todos os buckets do S3.

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

   Se você selecionar **Sim**, "Horário não atual" será selecionado automaticamente para Tempo de referência em"Etapa 2 do assistente Criar uma regra ILM" .

   > ⓘ O tempo não atual se aplica somente a objetos S3 em buckets habilitados para controle de versão. Ver"Operações em buckets, PutBucketVersioning" e"Gerenciar objetos com o S3 Object Lock" .

   Você pode usar esta opção para reduzir o impacto do armazenamento de objetos versionados filtrando por versões de objetos não atuais. Ver "Exemplo 4: regras e políticas do ILM para objetos versionados do S3" .

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

   Se você não configurar a filtragem avançada, a regra será aplicada a todos os objetos que corresponderem aos filtros básicos. Para obter mais informações sobre filtragem avançada, consulteUsar filtros avançados em regras de ILM eEspecifique vários tipos e valores de metadados .

7. Selecione **Continuar**. "Etapa 2 (Definir posicionamentos)"do assistente Criar uma regra ILM é exibido.

Usar filtros avançados em regras de ILM

A filtragem avançada permite que você crie regras de 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 de metadados
Tempo de ingestão	• é • não é • é antes • está em ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi ingerido. **Observação:** para evitar problemas de recursos ao ativar uma nova política de ILM, você pode usar o filtro avançado Tempo de ingestão em qualquer regra que possa alterar a localização de um grande número de objetos existentes. Defina o tempo de ingestão como 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	• é igual a • não é igual a • contém • não contém • começa com • não começa com • termina com • não termina com	Toda ou parte de uma chave de objeto S3 exclusiva. Por exemplo, você pode querer combinar objetos que terminam com `.txt` ou comece com `test-object/` .
Último horário de acesso	• é • não é • é antes • está em ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado). **Nota:** Se você planeja"usar último horário de acesso" como um filtro avançado, as atualizações de hora do último acesso devem ser habilitadas para o bucket S3.
Restrição de localização (somente S3)	• é igual a • não é igual a	A região onde um bucket S3 foi criado. Use **ILM** > **Regiões** para definir as regiões que são mostradas. **Observação:** Um valor de us-east-1 corresponderá a objetos em buckets criados na região us-east-1, bem como a objetos em buckets que não têm região especificada. Ver "Configurar regiões (opcional e somente S3)" .

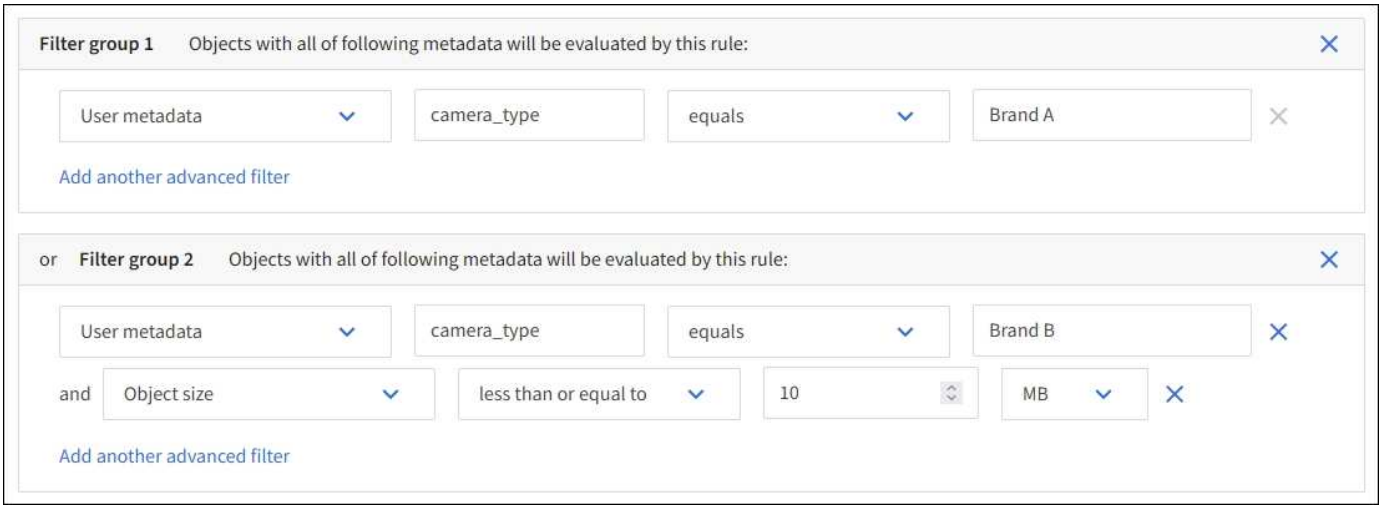
Tipo de metadados	Operadores suportados	Valor de metadados
Tamanho do objeto	• é igual a • não é igual a • menor que • menor ou igual a • maior que • maior ou igual a	O tamanho do objeto. A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.
Metadados do usuário	• contém • termina com • é igual a • existe • começa com • não contém • não termina com • não é igual a • não existe • não começa com	Par chave-valor, onde **Nome dos metadados do usuário** é a chave e **Valor dos metadados** é o valor. Por exemplo, para filtrar objetos que tenham metadados de usuário de `color=blue` , especifique `color` para **Nome de metadados do usuário**, `equals` para o operador, e `blue` para **Valor de metadados**. **Observação:** Os nomes de metadados do usuário não diferenciam maiúsculas de minúsculas; os valores de metadados do usuário diferenciam maiúsculas de minúsculas.
Tag de objeto (somente S3)	• contém • termina com • é igual a • existe • começa com • não contém • não termina com • não é igual a • não existe • não começa com	Par chave-valor, onde **Nome da tag do objeto** é a chave e **Valor da tag do objeto** é o valor. Por exemplo, para filtrar objetos que tenham uma tag de objeto de `Image=True` , especifique `Image` para **Nome da tag do objeto**, `equals` para o operador, e `True` para **valor da tag do objeto**. **Observação:** Os nomes de tags de objeto e os valores de tags de objeto diferenciam maiúsculas de minúsculas. Você deve inserir esses itens exatamente como foram definidos para o objeto.

Especifique vários tipos e valores de metadados

Ao definir a 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, selecione o tipo de metadados **Tamanho do objeto** e especifique 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.

Usar 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 Marca A ou Marca B como valor dos metadados do usuário camera_type. No entanto, a regra só se aplica aos objetos da Marca B que são menores que 10 MB.



Etapa 2 de 3: Definir posicionamentos

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

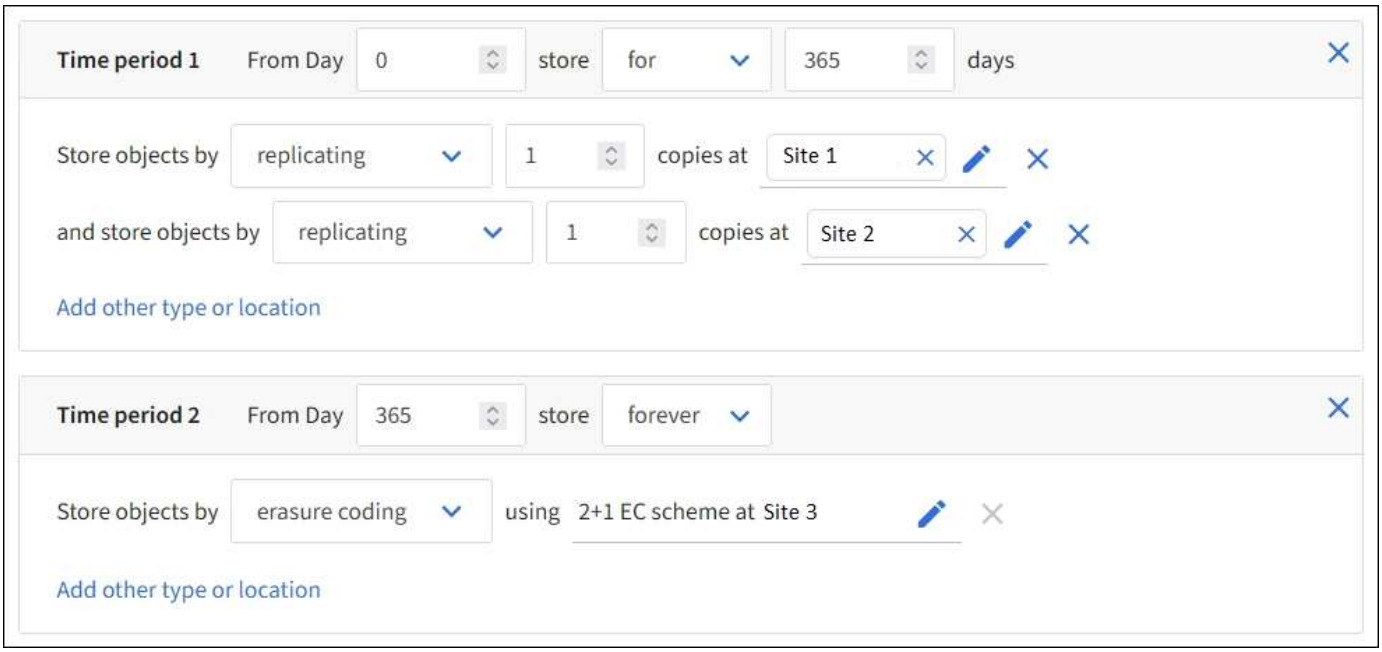
As capturas de tela mostradas são exemplos. Seus resultados podem variar dependendo da versão do StorageGRID .

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de posicionamento. Cada instrução de colocação se aplica 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 de cópias de objetos.

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

Neste exemplo, a regra ILM armazena uma cópia replicada no Site 1 e uma cópia replicada no Site 2 durante o primeiro ano. Após um ano, uma cópia codificada para eliminação 2+1 é feita e salva em apenas um site.



Passos

1. Para **Tempo de referência**, selecione o tipo de tempo a ser usado ao calcular o horário de início de uma instrução de posicionamento.

Opção	Descrição
Tempo de ingestão	O momento em que o objeto foi ingerido.
Último horário de acesso	A hora em que o objeto foi recuperado (lido ou visualizado) pela última vez. Para usar esta opção, as atualizações do Último horário de acesso devem ser habilitadas para o bucket S3. Consulte "Usar a hora do último acesso nas regras do ILM" .
Tempo de criação definido pelo usuário	Um tempo especificado em metadados definidos pelo usuário.
Tempo não atual	"Tempo não atual" é selecionado automaticamente se você selecionou **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" em"Etapa 1 do assistente Criar uma regra ILM" .

   Se você quiser criar uma regra *compatível*, selecione **Tempo de ingestão**. Consulte "Gerenciar objetos com o S3 Object Lock" .

2. Na seção **Período de tempo e posicionamentos**, insira um horário de início e uma duração para o primeiro período de tempo.

   Por exemplo, você pode querer especificar onde armazenar objetos durante o primeiro ano (*A partir do dia 0, armazenar por 365 dias*). Pelo menos uma instrução deve começar no dia 0.

3. Se você quiser criar cópias replicadas:

a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.

b. Selecione o número de cópias que você deseja fazer.

   Um aviso aparecerá 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. Consulte "Por que você não deve usar replicação de cópia única" .

   Para evitar o risco, faça uma ou mais das seguintes ações:

   - Aumentar o número de cópias para o período.
   - Adicione cópias a outros pools de armazenamento ou a um pool de armazenamento em nuvem.
   - Selecione **codificação de eliminação** em vez de **replicação**.

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

c. No campo **cópias em**, selecione os pools de armazenamento que deseja adicionar.

   Se você especificar apenas um pool de armazenamento, esteja ciente de que o StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se sua grade incluir três nós de armazenamento e você selecionar 4 como o número de cópias, apenas três cópias serão feitas, uma cópia para cada nó de armazenamento.

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

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

   - 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 armazenamento, uma cópia do objeto será armazenada em cada pool de armazenamento.
   - Se o número de cópias for menor que o número de pools de armazenamento, uma cópia será armazenada no site de ingestão e, em seguida, o sistema distribui as cópias restantes para manter o uso do disco entre os pools equilibrado, garantindo que nenhum site receba mais de uma cópia de um objeto.
   - Se os pools de armazenamento se sobrepuserem (contiverem os mesmos nós de armazenamento), todas as cópias do objeto poderão ser salvas em apenas um site. Por esse motivo, não especifique o pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) e outro pool de armazenamento.

4. Se você quiser criar uma cópia codificada para eliminação:

   a. Na lista suspensa **Armazenar objetos por**, selecione **codificação de eliminação**.

      A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

   b. Se você não adicionou um filtro de tamanho de objeto para um valor maior que 200 KB, selecione **Anterior** para retornar à Etapa 1. Em seguida, selecione **Adicionar um filtro avançado** e defina um filtro **Tamanho do objeto** para qualquer valor maior que 200 KB.

   c. Selecione o pool de armazenamento que deseja adicionar e o esquema de codificação de eliminação

que deseja usar.

O local de armazenamento de uma cópia codificada para eliminação inclui o nome do esquema de codificação para eliminação, seguido pelo nome do pool de armazenamento.

Os esquemas de codificação de eliminação disponíveis são limitados pelo número de nós de armazenamento no pool de armazenamento selecionado. UM `Recommended` O emblema aparece ao lado dos esquemas que fornecem o"melhor proteção ou menor sobrecarga de armazenamento" .

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

> As exclusões de objetos ocorrem com base nas seguintes configurações:
>
> - Os objetos são excluídos automaticamente no final do período de tempo final, a menos que outro período de tempo termine com **para sempre**.
> - Dependendo de"configurações de período de retenção de bucket e locatário" , os objetos podem não ser excluídos mesmo que o período de retenção do ILM termine.

6. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:
   a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.
   b. Selecione o campo **cópias em** e, em seguida, selecione um Pool de Armazenamento em Nuvem.

      Ao usar pools de armazenamento em nuvem, tenha estas regras em mente:

      - Não é possível selecionar mais de um Cloud Storage Pool em uma única instrução de posicionamento. Da mesma forma, você não pode selecionar um Cloud Storage Pool e um pool de armazenamento na mesma instrução de posicionamento.
      - Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro aparece se você definir **Cópias** como 2 ou mais.
      - Não é possível armazenar mais de uma cópia de objeto em nenhum 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 Cloud Storage Pool ao mesmo tempo em que ele está sendo armazenado como cópias replicadas ou codificadas para eliminação no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de posicionamento para o período de tempo, para que possa especificar o número e os tipos de cópias para cada local.

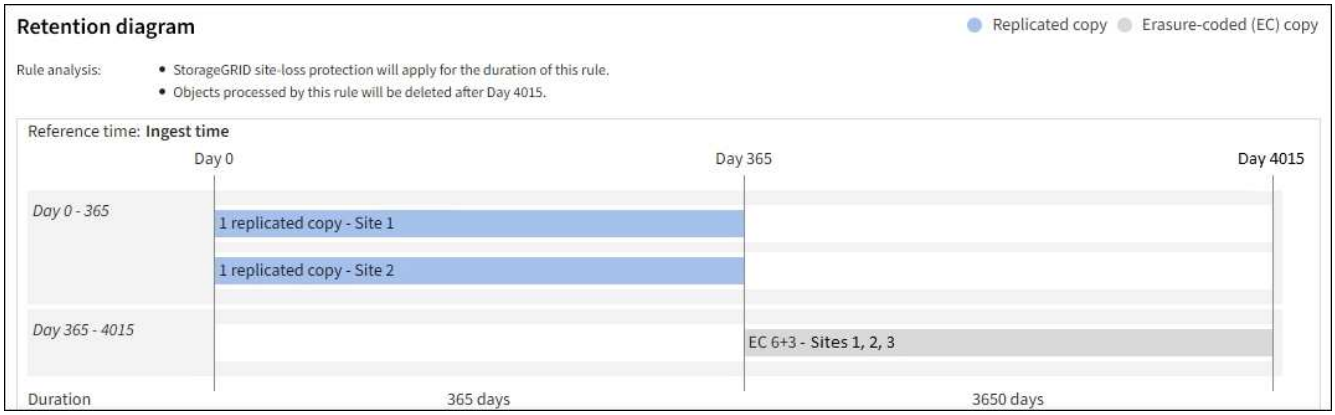
7. No diagrama de retenção, confirme suas instruções de posicionamento.

   Neste exemplo, a regra ILM armazena uma cópia replicada no Site 1 e uma cópia replicada no Site 2 durante o primeiro ano. Após um ano e por mais 10 anos, uma cópia codificada para eliminação 6+3 será salva em três locais. Após 11 anos no total, os objetos serão excluídos do StorageGRID.

   A seção Análise de regras do diagrama de retenção afirma:

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

Consulte "Ative a proteção contra perda de site."



8. Selecione **Continuar**. "Etapa 3 (Selecionar comportamento de ingestão)"do assistente Criar uma regra ILM é exibido.

Usar a hora do último acesso nas regras do ILM

Você pode usar o Último horário de acesso como horário de referência em uma regra do ILM. Por exemplo, você pode querer deixar objetos que foram visualizados nos últimos três meses em Nós de Armazenamento locais, enquanto move objetos que não foram visualizados recentemente para um local externo. Você também pode usar a Hora do último acesso como um filtro avançado se quiser que uma regra do ILM se aplique somente a objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

Antes de usar o Último horário de acesso em uma regra do ILM, revise as seguintes considerações:

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

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

- Ao usar o Último horário de acesso como um filtro avançado ou como um horário de referência, você deve habilitar as atualizações do último horário de acesso para os buckets do S3. Você pode usar o"Gerente de inquilinos" ou o"API de gerenciamento de inquilinos" .

  As atualizações do último horário de acesso são desabilitadas por padrão para buckets do S3.

  Esteja ciente de que habilitar atualizações de horário do último acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impacto no desempenho ocorre porque o StorageGRID deve atualizar os objetos com novos registros de data e hora sempre que os objetos são recuperados.

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

Tipo de solicitação	Se o último horário de acesso é atualizado quando as atualizações do último horário de acesso são desabilitadas	Se o último horário de acesso é atualizado quando as atualizações do último horário de acesso são habilitadas
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
Solicitação para concluir um upload multiparte	Sim, para o objeto montado	Sim, para o objeto montado

Etapa 3 de 3: Selecione o comportamento de ingestão

A etapa **Selecionar comportamento de ingestão** do assistente Criar regra ILM permite que você escolha como os objetos filtrados por esta regra serão protegidos à medida que são ingeridos.

Sobre esta tarefa

O StorageGRID pode fazer cópias provisórias e enfileirar os objetos para avaliação posterior do ILM, ou pode fazer cópias para atender às instruções de posicionamento da regra imediatamente.

Passos

1. Selecione o"comportamento de ingestão" para usar.

   Para obter mais informações, consulte "Vantagens, desvantagens e limitações das opções de ingestão" .

   > Você não pode usar a opção Balanceado ou Estrito se a regra usar um destes posicionamentos:
   >
   > - Um pool de armazenamento em nuvem no dia 0
   > - Um pool de armazenamento em nuvem quando a regra usa um horário de criação definido pelo usuário como horário de referência
   >
   > Ver "Exemplo 5: regras e política do ILM para comportamento de ingestão estrita" .

2. Selecione **Criar**.

   A regra ILM é criada. A regra não se torna ativa até que seja adicionada a um"Política de ILM" e essa política é ativada.

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

Criar uma regra ILM padrão

Antes de criar uma política de ILM, você deve criar uma regra padrão para colocar quaisquer objetos que não correspondam a outra regra na política. A regra padrão não pode usar nenhum filtro. Ele deve ser aplicado a todos os locatários, todos os buckets e todas as versões de objetos.

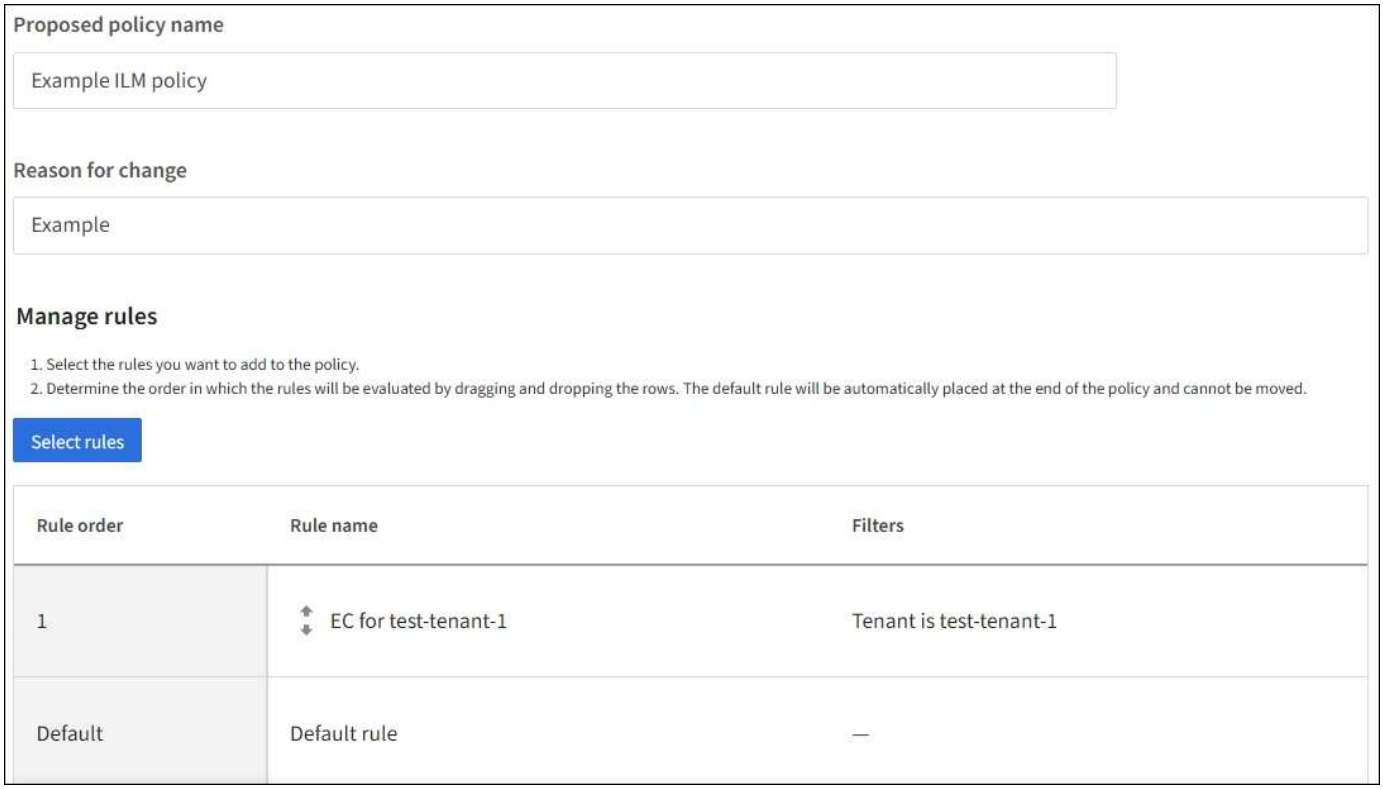
Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

A regra padrão é a última regra a ser avaliada em uma política de ILM, portanto, ela não pode usar nenhum filtro. As instruções de posicionamento da regra padrão são aplicadas a todos os objetos que não correspondem a outra regra na política.

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



Ao criar a regra padrão, tenha em mente estes requisitos:

- A regra padrão será automaticamente colocada como a última regra quando você adicioná-la a uma política.
- A regra padrão não pode usar nenhum filtro básico ou avançado.
- A regra padrão deve ser aplicada a todas as versões do objeto.
- A regra padrão deve criar cópias replicadas.

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

- Em geral, a regra padrão deve manter objetos para sempre.
- Se você estiver usando (ou planeja habilitar) a configuração global de Bloqueio de Objeto do S3, a regra padrão deverá ser compatível.

Passos

1. Selecione **ILM** > **Regras**.
2. Selecione **Criar**.

   A etapa 1 (Inserir detalhes) do assistente Criar regra ILM é exibida.

3. Insira um nome exclusivo para a regra no campo **Nome da regra**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.
5. Deixe o campo **Contas de inquilinos** em branco.

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

6. Deixe a seleção suspensa Nome do bucket como **aplica-se a todos os buckets**.

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

7. Mantenha a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões mais antigas de objetos (em buckets do S3 com controle de versão habilitado)?"
8. Não adicione filtros avançados.

   A regra padrão não pode especificar nenhum filtro.

9. Selecione **Avançar**.

   A etapa 2 (Definir posicionamentos) é exibida.

10. Para Tempo de referência, selecione qualquer opção.

    Se você mantivesse a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões mais antigas do objeto?" O tempo não atual não será incluído na lista suspensa. A regra padrão deve aplicar todas as versões do objeto.

11. Especifique as instruções de posicionamento 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 retém objetos para sempre. Você deve confirmar se esse é o comportamento esperado.
    - A regra padrão deve criar cópias replicadas.

    Não use uma regra que crie cópias codificadas para eliminação como regra padrão para uma política. As regras de codificação de eliminação devem incluir o filtro avançado **Tamanho do objeto (MB) maior que 200 KB** para evitar que objetos menores sejam codificados para eliminação.

- Se você estiver usando (ou planeja habilitar) a configuração global de bloqueio de objeto do S3, a regra padrão deve ser compatível:
  - Ele deve criar pelo menos duas cópias de objetos replicados ou uma cópia codificada para eliminação.
  - Essas cópias devem existir nos Nós de Armazenamento durante toda a duração de cada linha nas instruções de posicionamento.
  - Cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
  - Pelo menos uma linha das instruções de posicionamento deve começar no dia 0, usando o tempo de ingestão como tempo de referência.
  - Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

12. Observe o diagrama de retenção para confirmar suas instruções de posicionamento.
13. Selecione **Continuar**.

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

14. Selecione a opção de ingestão a ser usada e selecione **Criar**.

Gerenciar políticas de ILM

Usar políticas de ILM

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

> Uma política de ILM configurada incorretamente pode resultar em perda irrecuperável de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Política ILM padrão

Quando você instala o StorageGRID e adiciona sites, uma política de ILM padrão é criada automaticamente, da seguinte maneira:

- Se sua grade contiver um site, a política padrão conterá uma regra padrão que replica duas cópias de cada objeto naquele site.
- Se sua grade contiver mais de um site, a regra padrão replicará uma cópia de cada objeto em cada site.

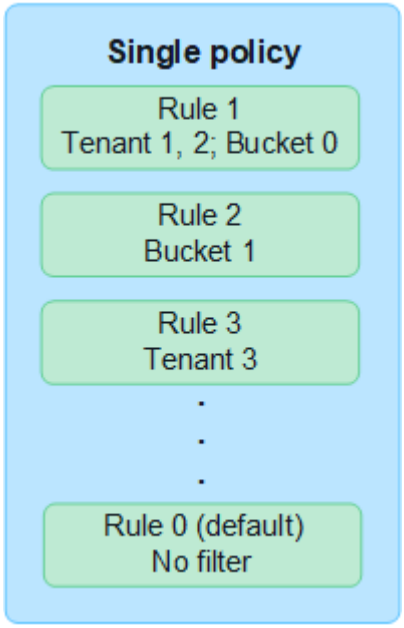
Se a política padrão não atender aos seus requisitos de armazenamento, você poderá criar suas próprias regras e políticas. Ver"Criar uma regra ILM" e"Criar uma política de ILM" .

Uma ou muitas políticas de ILM ativas?

Você pode ter uma ou mais políticas de ILM ativas por vez.

Uma política

Se sua grade usar um esquema simples de proteção de dados com poucas regras específicas de locatário e de bucket, use uma única política de ILM ativa. As regras do ILM podem conter filtros para gerenciar diferentes buckets ou locatários.



Quando você tem apenas uma política e os requisitos de um locatário mudam, você deve criar uma nova política de ILM ou clonar a política existente para aplicar as alterações, simular e, em seguida, ativar a nova política de ILM. Alterações na política do ILM podem resultar em movimentações de objetos que podem levar muitos dias e causar latência no sistema.

Políticas múltiplas

Para fornecer diferentes opções de qualidade de serviço aos inquilinos, você pode ter mais de uma apólice ativa ao mesmo tempo. Cada política pode gerenciar locatários, buckets S3 e objetos específicos. Quando você aplica ou altera uma política para um conjunto específico de locatários ou objetos, as políticas aplicadas a outros locatários e objetos não são afetadas.

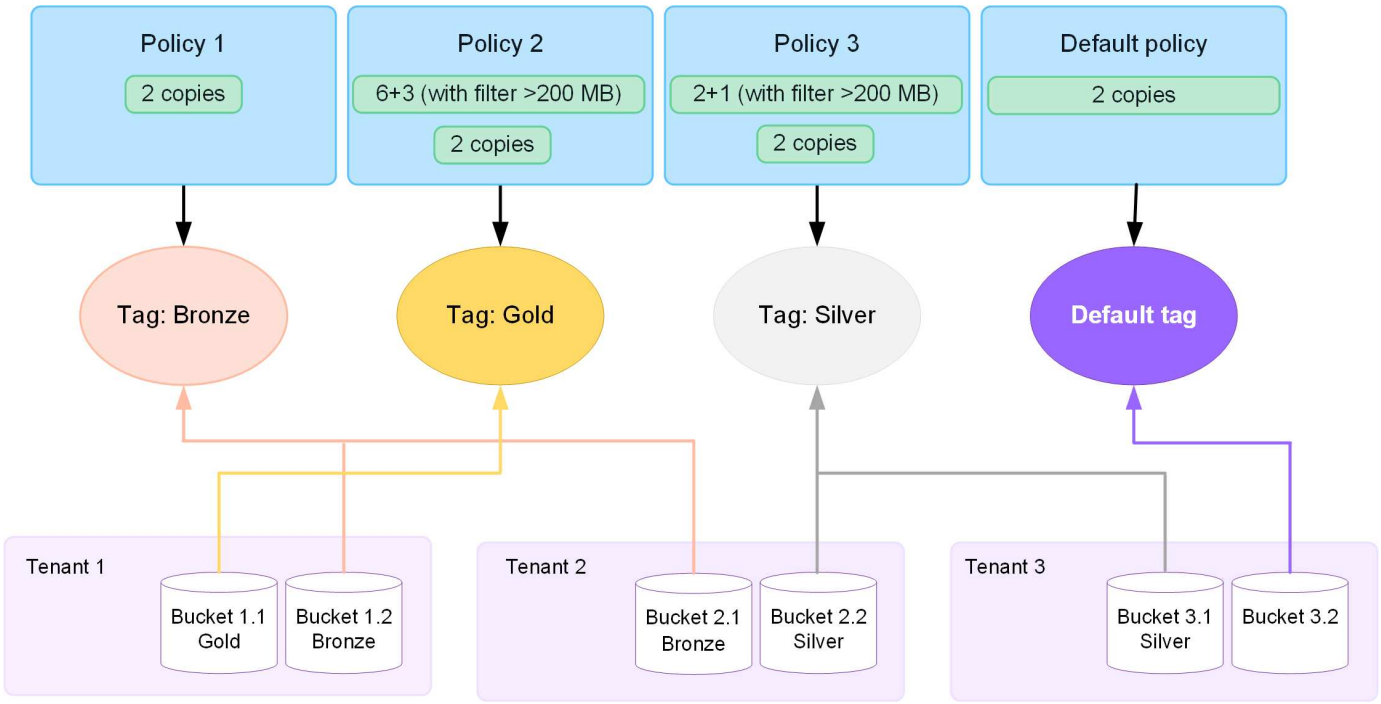
Tags de política do ILM

Se você quiser permitir que os locatários alternem facilmente entre várias políticas de proteção de dados por bucket, use várias políticas de ILM com *tags de política de ILM*. Você atribui cada política de ILM a uma tag e, em seguida, os locatários marcam um bucket para aplicar a política a esse bucket. Você pode definir tags de política do ILM somente em buckets do S3.

Por exemplo, você pode ter três tags chamadas Ouro, Prata e Bronze. Você pode atribuir uma política de ILM a cada tag, com base em quanto tempo e onde essa política armazena objetos. Os inquilinos podem escolher qual política usar marcando seus buckets. Um bucket marcado como Gold é gerenciado pela política Gold e recebe o nível Gold de proteção de dados e desempenho.

Tag de política ILM padrão

Uma tag de política ILM padrão é criada automaticamente quando você instala o StorageGRID. Cada grade deve ter uma política ativa atribuída à tag Padrão. A política padrão se aplica a todos os buckets S3 não marcados.



Como uma política de ILM avalia objetos?

Uma política de ILM ativa controla o posicionamento, a duração e a proteção de dados dos objetos.

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

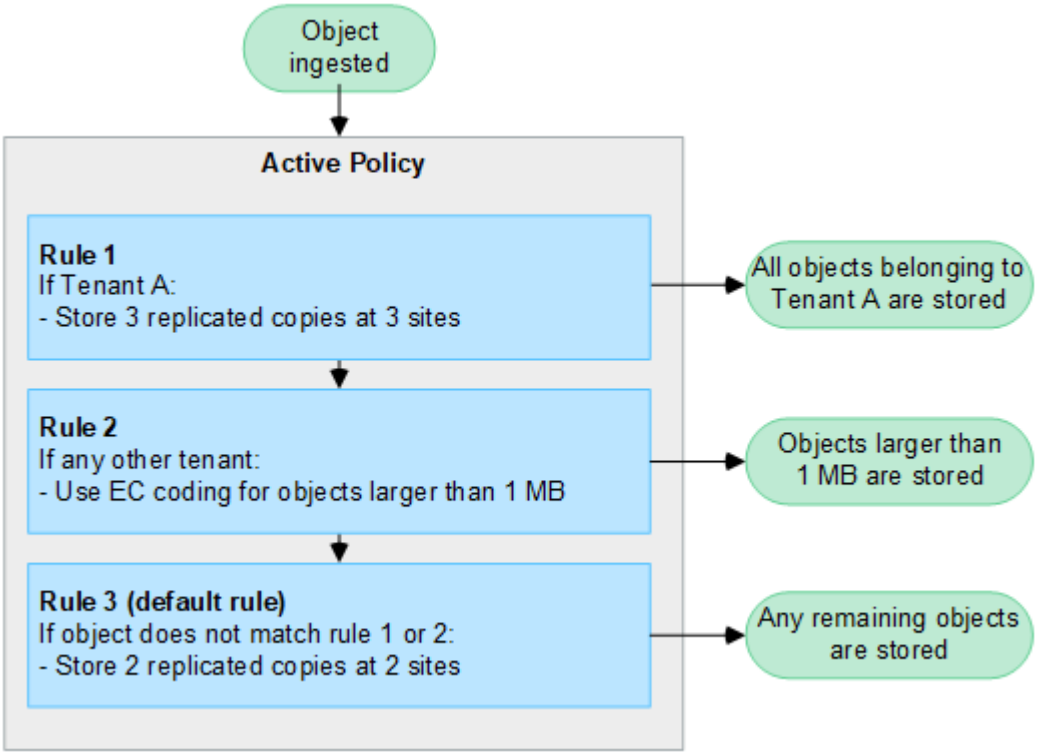
1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de posicionamento dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto será avaliado em relação a cada regra subsequente na política até que uma correspondência seja feita.
3. Se nenhuma regra corresponder a um objeto, o comportamento de ingestão e as instruções de posicionamento da regra padrão na política serão aplicados. A regra padrão é a última regra em uma política. A regra padrão deve ser aplicada a todos os locatários, todos os buckets do S3 e todas as versões de objeto, e não pode usar nenhum filtro avançado.

Exemplo de política de ILM

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

- **Regra 1: Cópias replicadas para o inquilino A**
  - Combine todos os objetos pertencentes ao Locatário A.
  - Armazene esses objetos como três cópias replicadas em três locais.
  - Objetos pertencentes a outros inquilinos não são correspondidos pela Regra 1, então eles são avaliados de acordo com a Regra 2.
- **Regra 2: Codificação de eliminação para objetos maiores que 1 MB**
  - Corresponda a todos os objetos de outros locatários, mas somente se eles forem maiores que 1 MB. Esses objetos maiores são armazenados usando codificação de eliminação 6+3 em três locais.

    - Não corresponde a objetos de 1 MB ou menores, portanto esses objetos são avaliados de acordo com a Regra 3.
- **Regra 3: 2 cópias para 2 data centers** (padrão)
    - É a última regra padrão da política. Não utiliza filtros.
    - Faça duas cópias replicadas de todos os objetos não correspondidos pela Regra 1 ou Regra 2 (objetos que não pertencem ao Locatário A e que têm 1 MB ou menos).



O que são políticas ativas e inativas?

Cada sistema StorageGRID deve ter pelo menos uma política de ILM ativa. Se você quiser ter mais de uma política de ILM ativa, crie tags de política de ILM e atribua uma política a cada tag. Os locatários então aplicam tags aos buckets do S3. A política padrão é aplicada a todos os objetos em buckets que não têm uma tag de política atribuída.

Ao criar uma política de ILM pela primeira vez, você seleciona uma ou mais regras de ILM e as organiza em uma ordem específica. Depois de simular a política para confirmar seu comportamento, você a ativa.

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

Se você ativar mais de uma política de ILM por vez e os locatários aplicarem tags de política aos buckets do S3, os objetos em cada bucket serão gerenciados de acordo com a política atribuída à tag.

Um sistema StorageGRID rastreia o histórico de políticas que foram ativadas ou desativadas.

Considerações para a criação de uma política de ILM

- Use somente a política fornecida pelo sistema, a política de cópias da Linha de Base 2, em sistemas de teste. Para o StorageGRID 11.6 e versões anteriores, a regra Fazer 2 cópias nesta política usa o pool de armazenamento Todos os nós de armazenamento, que contém todos os sites. Se o seu sistema

StorageGRID tiver mais de um site, duas cópias de um objeto poderão ser colocadas no mesmo site.

> O pool de armazenamento All Storage Nodes é criado automaticamente durante a instalação do StorageGRID 11.6 e versões anteriores. Se você atualizar para uma versão posterior do StorageGRID, o pool Todos os nós de armazenamento ainda existirá. Se você instalar o StorageGRID 11.7 ou posterior como uma nova instalação, o pool Todos os nós de armazenamento não será criado.

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

Criar políticas de ILM

Crie uma ou mais políticas de ILM para atender aos seus requisitos de qualidade de serviço.

Ter uma política de ILM ativa permite que você aplique as mesmas regras de ILM a todos os locatários e buckets.

Ter várias políticas de ILM ativas permite que você aplique as regras de ILM apropriadas a locatários e buckets específicos para atender a vários requisitos de qualidade de serviço.

Criar uma política de ILM

Sobre esta tarefa

Antes de criar sua própria política, verifique se o"política ILM padrão" não atende aos seus requisitos de armazenamento.

> Use somente as políticas fornecidas pelo sistema, 2 cópias da Política (para grades de um site) ou 1 cópia por site (para grades de vários sites), em sistemas de teste. Para o StorageGRID 11.6 e versões anteriores, a regra padrão nesta política usa o pool de armazenamento Todos os nós de armazenamento, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto poderão ser colocadas no mesmo site.

Se o"a configuração global de bloqueio de objeto S3 foi habilitada" , você deve garantir que a política do ILM esteja em conformidade com os requisitos dos buckets que têm o Bloqueio de Objeto S3 habilitado. Nesta seção, siga as instruções que mencionam ter o S3 Object Lock habilitado.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .
- Você tem"criou regras ILM" com base na ativação do bloqueio de objeto S3.

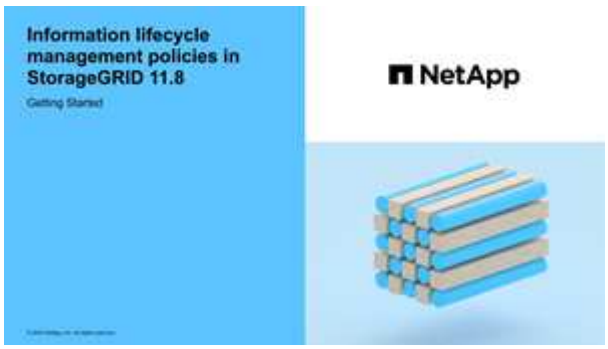
  Bloqueio de objeto S3 não habilitado

  - Você tem"criou as regras do ILM" que você deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e, em seguida, editar a política para adicionar as novas regras.
  - Você tem"criou uma regra ILM padrão" que não contém nenhum filtro.

  Bloqueio de objeto S3 habilitado

  - O"a configuração global de bloqueio de objeto S3 já está habilitada" para o sistema StorageGRID .
  - Você tem"criou as regras ILM compatíveis e não compatíveis" que você deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e, em seguida, editar a política para adicionar as novas regras.
  - Você tem"criou uma regra ILM padrão" para a política que está em conformidade.

- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral das políticas do ILM"



Veja também "Usar políticas de ILM" .

Passos

1. Selecione **ILM** > **Políticas**.

   Se a configuração global de Bloqueio de Objeto do S3 estiver habilitada, a página de políticas do ILM indicará quais regras do ILM são compatíveis.

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

Criar nova política

a. Selecione **Criar política**.

Clonar política existente

a. Marque a caixa de seleção da política com a qual deseja começar e selecione **Clonar**.

Editar política existente

a. Se uma política estiver inativa, você poderá editá-la. Marque a caixa de seleção da política inativa com a qual deseja começar e selecione **Editar**.

3. No campo **Nome da política**, insira um nome exclusivo para a política.
4. Opcionalmente, no campo **Motivo da alteração**, insira o motivo pelo qual você está criando uma nova política.
5. Para adicionar regras à política, selecione **Selecionar regras**. Selecione um nome de regra para visualizar as configurações dessa regra.

   Se você estiver clonando uma política:

   - As regras usadas pela política que você está clonando são selecionadas.
   - Se a política que você está clonando usou alguma regra sem filtros que não fosse a regra padrão, você será solicitado a remover todas, exceto uma dessas regras.
   - Se a regra padrão usou um filtro, você será solicitado a selecionar uma nova regra padrão.
   - Se a regra padrão não for a última regra, você poderá movê-la para o final da nova política.

Bloqueio de objeto S3 não habilitado

a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **Página de regras do ILM**.

   A regra padrão se aplica a qualquer objeto que não corresponda a outra regra na política. A regra padrão não pode usar nenhum filtro e é sempre avaliada por último.

   > Não use a regra Fazer 2 cópias como regra padrão para uma política. A regra Fazer 2 cópias usa um único pool de armazenamento, Todos os nós de armazenamento, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto poderão ser colocadas no mesmo site.

Bloqueio de objeto S3 habilitado

a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **Página de regras do ILM**.

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

   > Não use a regra Fazer 2 cópias como regra padrão para uma política. A regra Fazer 2 cópias usa um único pool de armazenamento, Todos os nós de armazenamento, que contém todos os sites. Se você usar essa regra, várias cópias de um objeto poderão ser colocadas no mesmo site.

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

   Por exemplo, você pode querer usar um Cloud Storage Pool para armazenar objetos em buckets que não tenham o S3 Object Lock habilitado.

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

Veja também "Exemplo 7: Política ILM compatível para bloqueio de objeto S3" .

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

   A janela Criar uma política agora lista as regras que você selecionou. A regra padrão está no final, com as outras regras acima dela.

   Se o Bloqueio de Objeto S3 estiver habilitado e você também tiver selecionado uma regra "padrão" não compatível, essa regra será adicionada como a penúltima regra na política.

   > Um aviso aparece se alguma regra não retém objetos para sempre. Ao ativar esta política, você deve confirmar que deseja que o StorageGRID exclua objetos quando as instruções de posicionamento da regra padrão expirarem (a menos que um ciclo de vida do bucket mantenha os objetos por um período mais longo).

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

   Você não pode mover a regra padrão. Se o Bloqueio de Objeto S3 estiver habilitado, você também não poderá mover a regra "padrão" não compatível, caso uma tenha sido selecionada.

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

9. Conforme necessário, selecione **Selecionar regras** para adicionar ou remover regras.
10. Quando terminar, selecione **Salvar**.
11. Repita essas etapas para criar políticas de ILM adicionais.
12. Simular uma política de ILM . Você deve sempre simular uma política antes de ativá-la para garantir que ela funcione conforme o esperado.

Simular uma política

Simule uma política em objetos de teste antes de ativar a política e aplicá-la aos seus dados de produção.

Antes de começar

- Você conhece o bucket/chave de objeto do S3 para cada objeto que deseja testar.

Passos

1. Usando um cliente S3 ou o"Console S3" , ingira os objetos necessários para testar cada regra.
2. Na página de políticas do ILM, marque a caixa de seleção da política e selecione **Simular**.
3. No campo **Objeto**, insira o S3 `bucket/object-key` para um objeto de teste. Por exemplo, `bucket-01/filename.png` .
4. Se o controle de versão do S3 estiver habilitado, opcionalmente insira um ID de versão para o objeto no campo **ID da versão**.
5. Selecione **Simular**.
6. Na seção Resultados da simulação, confirme se cada objeto foi correspondido pela regra correta.
7. Para determinar qual pool de armazenamento ou perfil de codificação de eliminação está em vigor, selecione o nome da regra correspondente para acessar a página de detalhes da regra.

> Revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Resultados

Quaisquer edições nas regras da política serão refletidas nos resultados da simulação e mostrarão a nova correspondência e a correspondência anterior. A janela Simular política retém os objetos que você testou até que você selecione **Limpar tudo** ou o ícone remover para cada objeto na lista de resultados da simulação.

Informações relacionadas

"Exemplos de simulações de políticas de ILM"

Ativar uma política

Quando você ativa uma única nova política de ILM, os objetos existentes e os objetos recém-ingeridos são gerenciados por essa política. Quando você ativa várias políticas, as tags de política do ILM atribuídas aos buckets determinam os objetos a serem gerenciados.

Antes de ativar uma nova política:

1. Simule a política para confirmar se ela se comporta conforme o esperado.
2. Revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Erros em uma política de ILM podem causar perda irrecuperável de dados.

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 entrar em vigor até que todos os nós da grade estejam disponíveis para receber a nova política. Em alguns casos, o sistema aguarda para implementar uma nova política ativa para garantir que os objetos da grade não sejam removidos acidentalmente. Especificamente:

- 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 ou a durabilidade dos dados**, essas alterações não serão implementadas até que todos os nós da grade estejam disponíveis. Por exemplo, se você ativar uma nova política que usa uma regra de duas cópias em vez de uma regra de três cópias, a nova política aparecerá na guia Política ativa, mas não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

Siga as etapas para ativar uma ou várias políticas:

Ativar uma política

Siga estas etapas se você tiver apenas uma política ativa. Se você já tiver uma ou mais políticas ativas e estiver ativando políticas adicionais, siga as etapas para ativar várias políticas.

1. Quando estiver pronto para ativar uma política, selecione **ILM** > **Políticas**.

   Como alternativa, você pode ativar uma única política na página **ILM** > **Tags de política**.

2. Na guia Políticas, marque a caixa de seleção da política que você deseja ativar e selecione **Ativar**.
3. Siga o passo apropriado:
   - Se uma mensagem de aviso solicitar que você confirme se deseja ativar a política, selecione **OK**.
   - Se uma mensagem de aviso contendo detalhes sobre a política for exibida:
     i. Revise os detalhes para garantir que a política gerenciará os dados conforme o esperado.
     ii. Se a regra padrão armazenar objetos por um número limitado de dias, revise o diagrama de retenção e digite esse número de dias na caixa de texto.
     iii. Se a regra padrão armazena objetos para sempre, mas uma ou mais outras regras têm retenção limitada, digite **sim** na caixa de texto.
     iv. Selecione **Ativar política**.

Ativar várias políticas

Para ativar várias políticas, você deve criar tags e atribuir uma política a cada tag.

> Quando várias tags estão em uso, se os locatários reatribuírem frequentemente tags de política aos buckets, o desempenho da grade poderá ser afetado. Se você tiver inquilinos não confiáveis, considere usar apenas a tag Padrão.

1. Selecione **ILM** > **Tags de política**.
2. Selecione **Criar**.
3. Na caixa de diálogo Criar tag de política, digite um nome de tag e, opcionalmente, uma descrição para a tag.

   > Os nomes e descrições das tags são visíveis para os inquilinos. Escolha valores que ajudarão os inquilinos a tomar uma decisão informada ao selecionar tags de política para atribuir aos seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

4. Selecione **Criar tag**.
5. Na tabela de tags de política do ILM, use o menu suspenso para selecionar uma política a ser atribuída à tag.
6. Se avisos aparecerem na coluna Limitações da política, selecione **Exibir detalhes da política** para revisá-la.
7. Garanta que cada política gerencie os dados conforme o esperado.
8. Selecione **Ativar políticas atribuídas**. Ou selecione **Limpar alterações** para remover a atribuição de política.

9. Na caixa de diálogo Ativar políticas com novas tags, revise as descrições de como cada tag, política e regra gerenciará objetos. Faça as alterações necessárias para garantir que as políticas gerenciem os objetos conforme o esperado.
10. Quando tiver certeza de que deseja ativar as políticas, digite **sim** na caixa de texto e selecione **Ativar políticas**.

Informações relacionadas

"Exemplo 6: Alterando uma política de ILM"

Exemplos de simulações de políticas de ILM

Os exemplos de simulações de políticas de ILM fornecem diretrizes para estruturar e modificar simulações para seu ambiente.

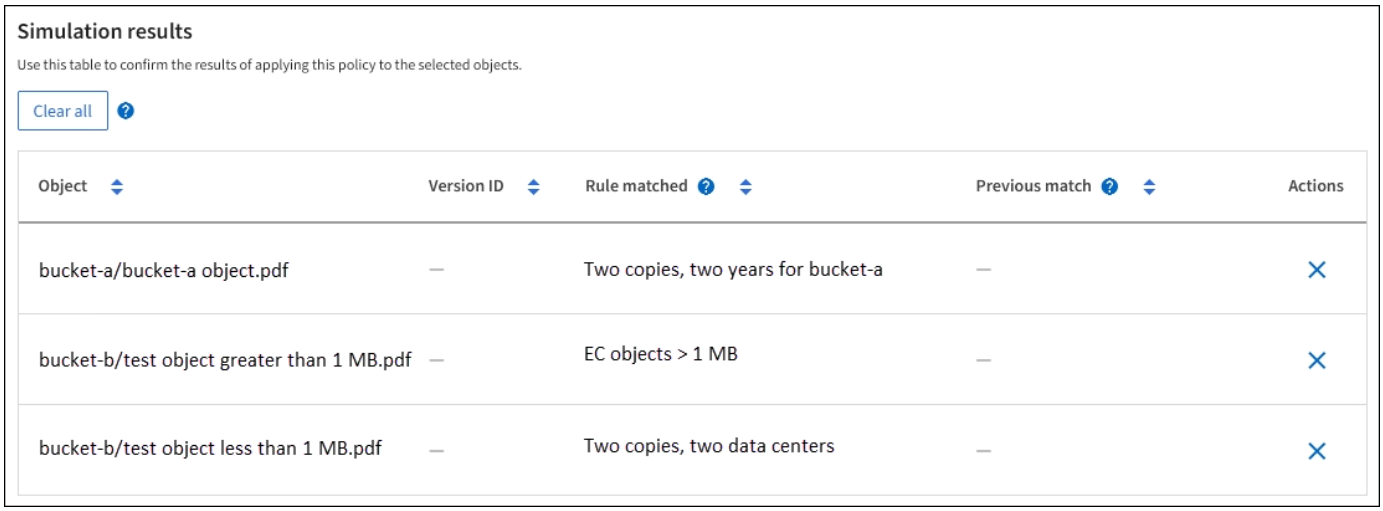
Exemplo 1: Verificar regras ao simular uma política de ILM

Este exemplo descreve como verificar regras ao simular uma política.

Neste exemplo, a **Política ILM de exemplo** está sendo simulada em relação aos objetos ingeridos em dois buckets. A política inclui três regras, a saber:

- A primeira regra, **Duas cópias, dois anos para o bucket-a**, aplica-se somente a objetos no bucket-a.
- A segunda regra, **Objetos EC > 1 MB**, se aplica a todos os buckets, mas filtra objetos maiores que 1 MB.
- A terceira regra, **Duas cópias, dois data centers**, é a regra padrão. Não inclui nenhum filtro e não usa o tempo de referência não atual.

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



Neste exemplo:

- `bucket-a/bucket-a object.pdf`correspondeu corretamente à primeira regra, que filtra objetos em `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf`está em `bucket-b`, então não correspondia à primeira regra. Em vez disso, ele foi correspondido corretamente pela segunda regra, que filtra objetos maiores que 1 MB.

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

Exemplo 2: Regras de reordenação ao simular uma política de ILM

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

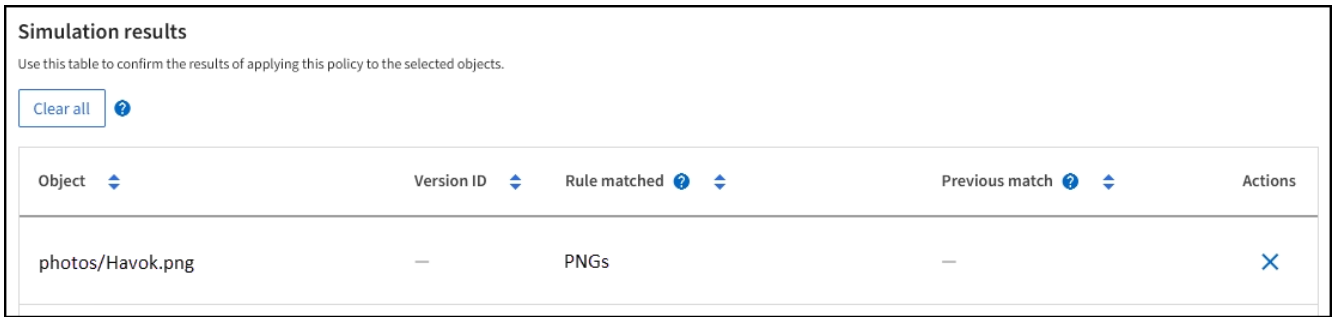
Neste exemplo, a política **Demo** está sendo simulada. Esta política, que visa encontrar objetos que tenham metadados de usuário series=x-men, inclui três regras, como segue:

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

Passos

1. Depois de adicionar as regras e salvar a política, selecione **Simular**.
2. No campo **Objeto**, insira o bucket/chave de objeto S3 para um objeto de teste e selecione **Simular**.

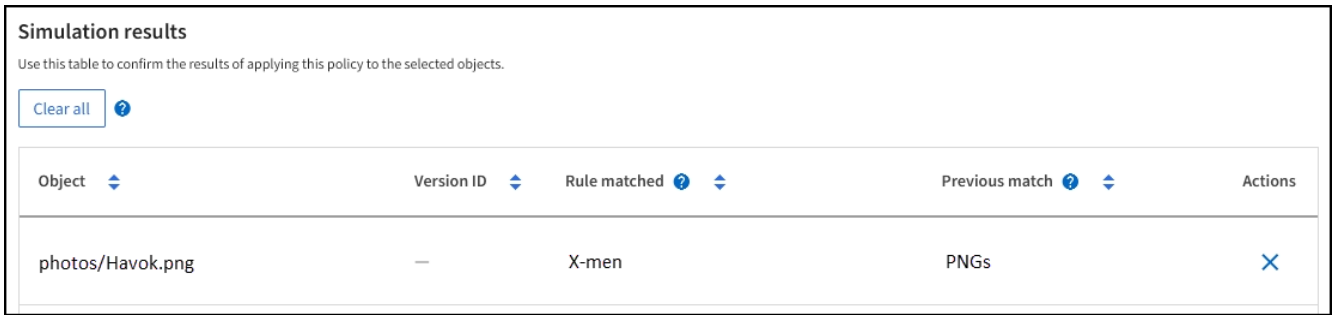
   Os resultados da simulação aparecem, mostrando que o `Havok.png` objeto foi correspondido pela regra **PNGs**.



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

3. Para resolver o problema, reordene as regras.
   a. Selecione **Concluir** para fechar a janela Simular política de ILM.
   b. Selecione **Editar** para editar a política.
   c. Arraste a regra **X-men** para o topo da lista.
   d. Selecione **Salvar**.
4. Selecione **Simular**.

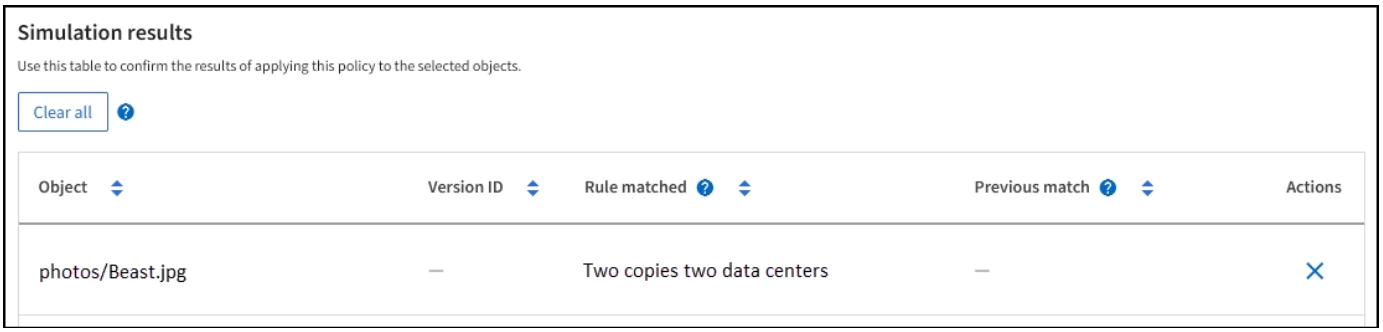
   Os objetos testados anteriormente são reavaliados em relação à política atualizada, e os novos resultados da simulação são exibidos. No exemplo, a coluna Regra correspondida mostra que o `Havok.png` o objeto agora corresponde à regra de metadados dos X-men, como esperado. A coluna Correspondência anterior mostra que a regra PNGs correspondeu ao objeto na simulação anterior.



Exemplo 3: Corrigir uma regra ao simular uma política de ILM

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 tem como objetivo encontrar objetos que tenham `series=x-men` metadados do usuário. No entanto, resultados inesperados ocorreram ao simular esta política contra o `Beast.jpg` objeto. Em vez de corresponder à regra de metadados dos X-men, o objeto correspondeu à regra padrão: Duas cópias de dois data centers.



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

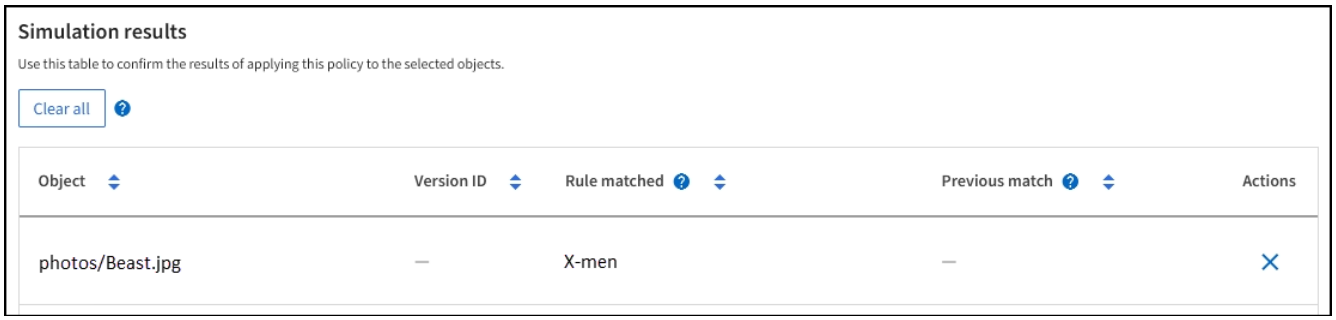
Passos

1. Selecione **Concluir** para fechar a caixa de diálogo Simular política. Na página de detalhes da política, selecione **Diagrama de retenção**. Em seguida, selecione **Expandir tudo** ou **Exibir detalhes** para cada regra, conforme necessário.
2. Revise a conta do locatário da regra, o tempo de referência e os critérios de filtragem.

   Por exemplo, suponha que os metadados da regra dos X-men foram inseridos como "x-men01" em vez de "x-men".

3. Para resolver o erro, corrija a regra da seguinte maneira:
   - Se a regra fizer parte da política, você poderá cloná-la ou removê-la da política e editá-la.
   - Se a regra fizer parte da política ativa, você deverá cloná-la. Você não pode editar ou remover uma regra da política ativa.
4. Execute a simulação novamente.

   Neste exemplo, a regra corrigida dos X-men agora corresponde à `Beast.jpg` objeto baseado no `series=x-men` metadados do usuário, conforme esperado.



Gerenciar tags de política do ILM

Você pode visualizar detalhes da tag de política do ILM, editar uma tag ou remover uma tag.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissões de acesso necessárias" .

Exibir detalhes da tag de política do ILM

Para visualizar os detalhes de uma tag:

1. Selecione **ILM** > **Tags de política**.
2. Selecione o nome da política na tabela. A página de detalhes da tag é exibida.
3. Na página de detalhes, visualize o histórico anterior das políticas atribuídas.
4. Visualize uma política selecionando-a.

Editar tag de política do ILM

> Os nomes e descrições das tags são visíveis para os inquilinos. Escolha valores que ajudarão os inquilinos a tomar uma decisão informada ao selecionar tags de política para atribuir aos seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

Para editar a descrição de uma tag existente:

1. Selecione **ILM** > **Tags de política**.
2. Selecione a caixa de seleção da tag e selecione **Editar**.

   Como alternativa, selecione o nome da tag. A página de detalhes da tag é exibida e você pode selecionar **Editar** nessa página.

3. Altere a descrição da tag conforme necessário
4. Selecione **Salvar**.

Remover tag de política ILM

Quando você remove uma tag de política, todos os buckets aos quais essa tag foi atribuída terão a política Padrão aplicada.

Para remover uma tag:

1. Selecione **ILM** > **Tags de política**.
2. Marque a caixa de seleção da tag e selecione **Remover**. Uma caixa de diálogo de confirmação é exibida.

   Como alternativa, selecione o nome da tag. A página de detalhes da tag é exibida e você pode selecionar **Remover** nessa página.

3. Selecione **Sim** para excluir a tag.

Verificar uma política de ILM com consulta de metadados de objeto

Depois de ativar uma política de ILM, ingira objetos de teste representativos no sistema StorageGRID e execute uma pesquisa de metadados do objeto para confirmar se as cópias estão sendo feitas conforme o esperado e colocadas nos locais corretos.

Antes de começar

Você tem um identificador de objeto, que pode ser um dos seguintes: * **UUID**: Identificador Universalmente Único do objeto. * **CBID**: O identificador exclusivo do objeto dentro do StorageGRID. Você pode obter o CBID de um objeto no log de auditoria. Digite o CBDID em letras maiúsculas. * **Chave de bucket e objeto S3**: Quando um objeto é ingerido por meio da interface S3, o aplicativo cliente usa uma combinação de chave de bucket e objeto para armazenar e identificar o objeto. Se o bucket do S3 tiver versão e você quiser consultar uma versão específica de um objeto do S3 usando o bucket e a chave do objeto, você terá o **ID da versão**.

Passos

1. Ingerir o objeto.
2. Selecione **ILM** > **Consulta de metadados do objeto**.
3. Digite o identificador do objeto no campo **Identificador**. Você pode inserir um UUID, CBID ou chave de objeto/bucket S3.
4. Opcionalmente, insira um ID de versão para o objeto (somente S3).
5. Selecione **Procurar**.

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

   - Metadados do sistema, como ID do objeto (UUID), tipo de resultado (objeto, marcador de exclusão, bucket S3) e tamanho lógico do objeto. Consulte a captura de tela de exemplo abaixo para obter mais detalhes.
   - Quaisquer pares de chave-valor de metadados de usuário personalizados associados ao objeto.
   - Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
   - Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.
   - Para cópias de objetos codificadas por eliminação, o local de armazenamento atual de cada fragmento.
   - Para cópias de objetos em um pool de armazenamento em nuvem, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
   - Para objetos segmentados e objetos multipartes, uma lista de segmentos de objetos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, somente os primeiros 100 segmentos são mostrados.

- Todos os metadados do objeto no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não têm garantia de persistência de uma versão para outra.

6. Confirme se o objeto está armazenado no(s) local(is) correto(s) e se é o tipo correto de cópia.

   Se a opção Auditoria estiver habilitada, você também poderá monitorar o log de auditoria para a mensagem Regras de objeto ORLM atendidas. A mensagem de auditoria do ORLM pode fornecer mais informações sobre o status do processo de avaliação do ILM, mas não pode fornecer informações sobre a exatidão do posicionamento dos dados do objeto ou a integridade da política do ILM. Você deve avaliar isso você mesmo. Para obter detalhes, consulte "Revisar logs de auditoria" .

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

A captura de tela a seguir é um exemplo. Seus resultados variarão dependendo da versão do StorageGRID .

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",
```


Informações relacionadas

"Usar API REST do S3"

Trabalhar com políticas e regras do ILM

À medida que seus requisitos de armazenamento mudam, pode ser necessário implementar políticas adicionais ou modificar as regras de ILM associadas a uma política. Você pode visualizar métricas do ILM para determinar o desempenho do sistema.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Ver políticas do ILM

Para visualizar políticas de ILM ativas e inativas e o histórico de ativação de políticas:

1. Selecione **ILM** > **Políticas**.
2. Selecione **Políticas** para visualizar uma lista de políticas ativas e inativas. A tabela lista o nome de cada política, as tags às quais a política está atribuída e se a política está ativa ou inativa.
3. Selecione **Histórico de ativação** para visualizar uma lista de datas de início e término de ativação das políticas.
4. Selecione um nome de política para visualizar os detalhes da política.

Se você visualizar os detalhes de uma política cujo status é Editado ou Excluído, uma mensagem será exibida explicando que você está visualizando a versão da política que estava ativa durante o período especificado e que desde então foi editada ou excluída.

Editar uma política de ILM

Você só pode editar uma política inativa. Se você quiser editar uma política ativa, desative-a ou crie um clone e edite o clone.

Para editar uma política:

1. Selecione **ILM** > **Políticas**.
2. Marque a caixa de seleção da política que você deseja editar e selecione **Editar**.
3. Edite a política seguindo as instruções em"Criar políticas de ILM" .
4. Simule a política antes de reativá-la.

Uma política de ILM configurada incorretamente pode resultar em perda irrecuperável de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Clonar uma política de ILM

Para clonar uma política ILM:

1. Selecione **ILM** > **Políticas**.
2. Marque a caixa de seleção da política que você deseja clonar e selecione **Clonar**.
3. Crie uma nova política começando com a política que você clonou seguindo as instruções em"Criar políticas de ILM" .

> Uma política de ILM configurada incorretamente pode resultar em perda irrecuperável de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Remover uma política de ILM

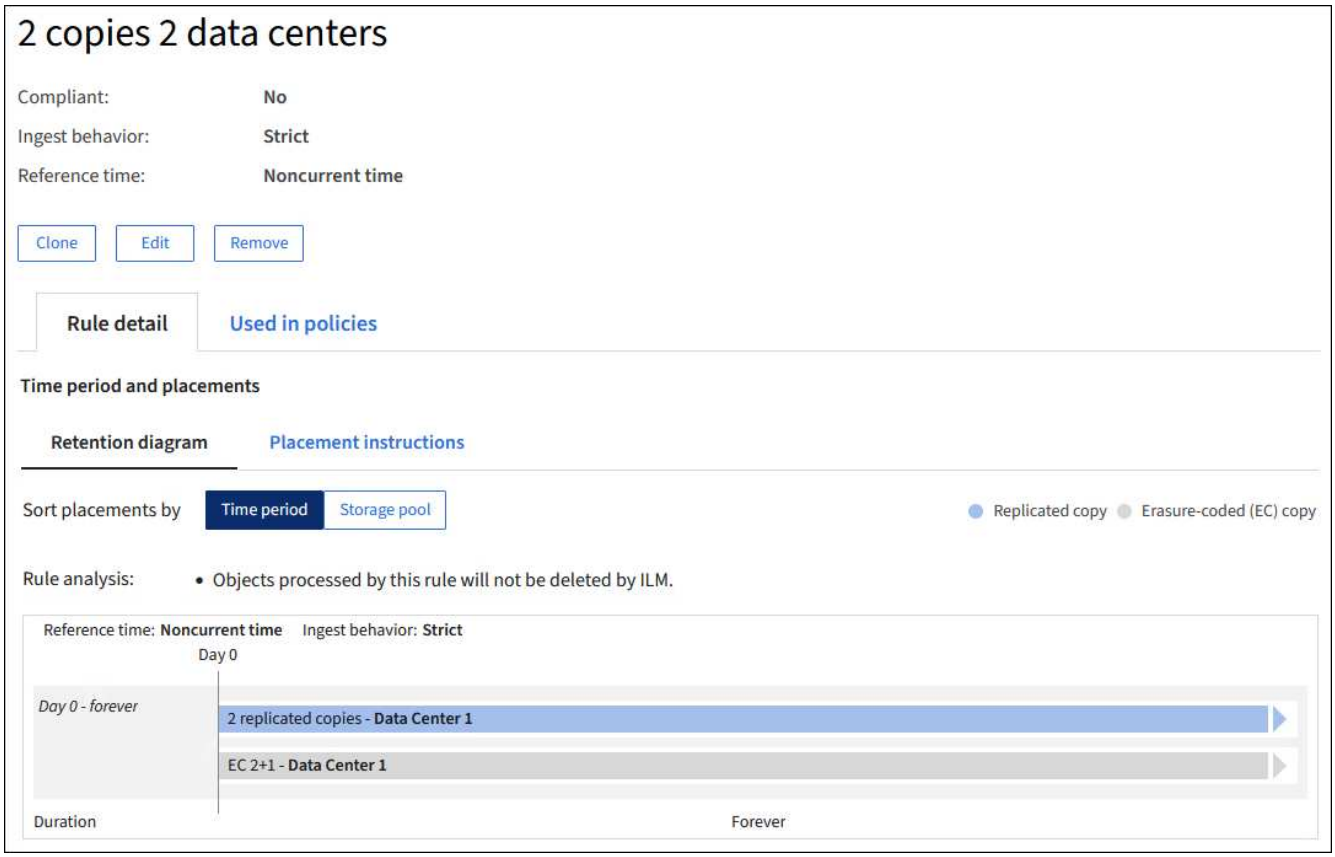
Você só pode remover uma política de ILM se ela estiver inativa. Para remover uma política:

1. Selecione **ILM** > **Políticas**.
2. Marque a caixa de seleção da política inativa que você deseja remover.
3. Selecione **Remover**.

Ver detalhes da regra do ILM

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

1. Selecione **ILM** > **Regras**.
2. Selecione o nome da regra cujos detalhes você deseja visualizar. Exemplo:



Além disso, você pode usar a página de detalhes para clonar, editar ou remover uma regra. Você não pode editar ou remover uma regra se ela for usada em qualquer política.

Clonar uma regra ILM

Você pode clonar uma regra existente se quiser criar uma nova regra que use algumas das configurações da regra existente. Se você precisar editar uma regra usada em qualquer política, clone a regra e faça alterações no clone. Depois de fazer alterações no clone, você pode remover a regra original da política e substituí-la pela versão modificada, conforme necessário.

> Não é possível clonar uma regra do ILM se ela foi criada usando o StorageGRID versão 10.2 ou anterior.

Passos

1. Selecione **ILM** > **Regras**.
2. Marque a caixa de seleção da regra que você deseja clonar e selecione **Clonar**. Como alternativa, selecione o nome da regra e, em seguida, selecione **Clonar** na página de detalhes da regra.
3. Atualize a regra clonada seguindo as etapas paraeditando uma regra ILM e"usando filtros avançados em regras ILM" .

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

Editar uma regra ILM

Pode ser necessário editar uma regra do ILM para alterar um filtro ou uma instrução de posicionamento.

Você não pode editar uma regra se ela for usada em qualquer política do ILM. Em vez disso, você pode clonar a regra e faça as alterações necessárias na cópia clonada.

> Uma política de ILM configurada incorretamente pode resultar em perda irrecuperável de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Passos

1. Selecione **ILM** > **Regras**.
2. Confirme se a regra que você deseja editar não é usada em nenhuma política do ILM.
3. Se a regra que você deseja editar não estiver em uso, marque a caixa de seleção da regra e selecione **Ações** > **Editar**. Como alternativa, selecione o nome da regra e selecione **Editar** na página de detalhes da regra.
4. Conclua as etapas do assistente Editar regra do ILM. Conforme necessário, siga os passos para "criando uma regra ILM" e "usando filtros avançados em regras ILM" .

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

Remover uma regra ILM

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

Passos

Para remover uma regra de ILM que está sendo usada atualmente em uma política ativa:

1. Clone a política.
2. Remova a regra ILM do clone da política.
3. Salve, simule e ative a nova política para garantir que os objetos estejam protegidos conforme o esperado.
4. Vá para as etapas para remover uma regra de ILM que está sendo usada atualmente em uma política inativa.

Para remover uma regra ILM que está sendo usada atualmente em uma política inativa:

1. Selecione a política inativa.
2. Remova a regra ILM da política ou remover a política .
3. Vá para as etapas para remover uma regra do ILM que não está sendo usada no momento.

Para remover uma regra ILM que não está sendo usada no momento:

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

Ver métricas do ILM

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

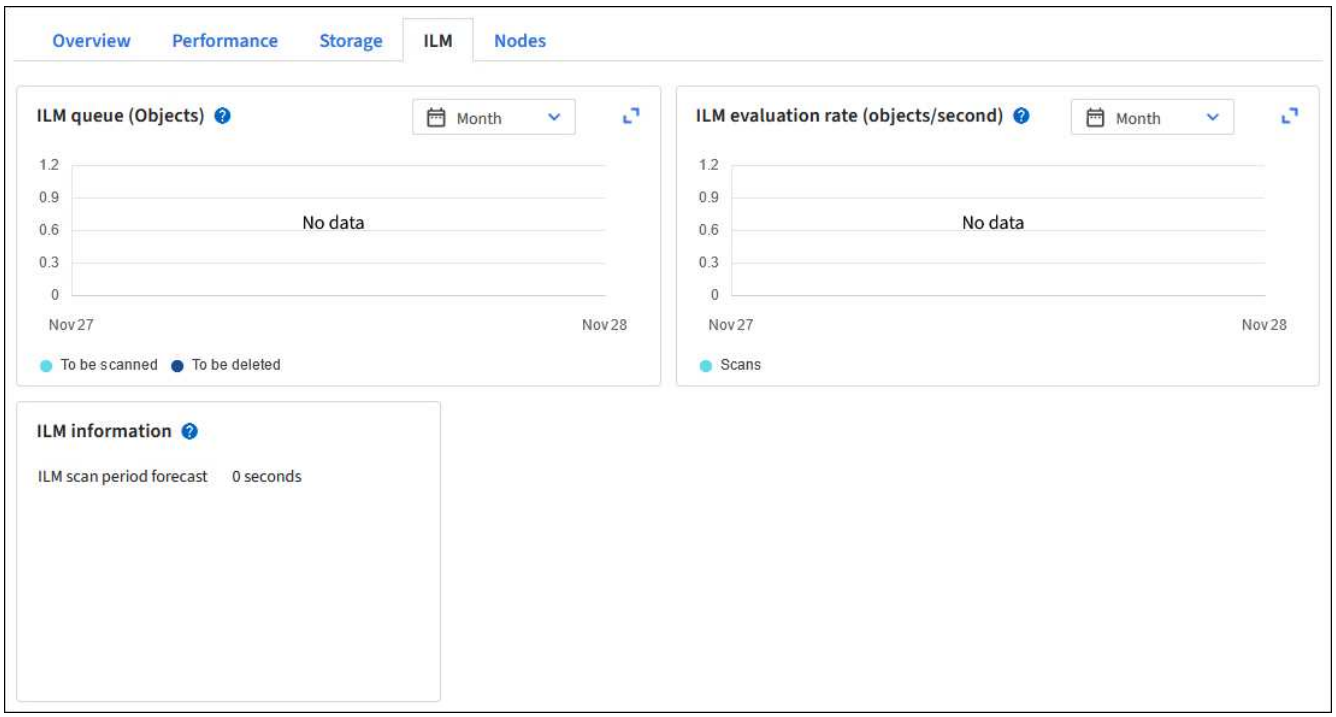
Passos

1. Selecione **Painel** > **ILM**.

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

2. Monitore as métricas na guia ILM.

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



Usar bloqueio de objeto S3

Gerenciar objetos com o S3 Object Lock

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

O que é o S3 Object Lock?

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

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

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

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

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

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

Modos de retenção

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

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

Configurações de retenção para versões de objeto

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

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

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

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

Configuração de retenção padrão para buckets

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

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

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

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

Comparando o bloqueio de objeto S3 com a conformidade legada

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

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

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

	Bloqueio de Objeto S3	**Conformidade (legado)**
Como o recurso é habilitado globalmente?	No Grid Manager, selecione **CONFIGURAÇÃO** > **Sistema** > **Bloqueio de Objeto S3**.	Não é mais suportado.
Como o recurso é habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto do S3 ao criar um novo bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API.	Não é mais suportado.
O controle de versão de bucket é suportado?	Sim. O controle de versão do bucket é necessário e é habilitado automaticamente quando o S3 Object Lock é habilitado para o bucket.	Não.

	Bloqueio de Objeto S3	Conformidade (legado)
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção para cada versão do objeto ou podem definir um período de retenção padrão para cada bucket.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção se aplica a todos os objetos no bucket.
O período de retenção pode ser alterado?	• No modo de conformidade, o período de retenção até a data para uma versão do objeto pode ser aumentado, mas nunca diminuído. • No modo de governança, usuários com permissões especiais podem diminuir ou até mesmo remover as configurações de retenção de um objeto.	O período de retenção de um bucket pode ser aumentado, mas nunca diminuído.
Onde a retenção legal é controlada?	Os usuários podem colocar ou retirar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no bucket e afeta todos os objetos no bucket.
Quando os objetos podem ser excluídos?	• No modo de conformidade, uma versão do objeto pode ser excluída após a data de retenção ser atingida, supondo que o objeto não esteja sob retenção legal. • No modo de governança, usuários com permissões especiais podem excluir um objeto antes que sua data de retenção seja atingida, supondo que o objeto não esteja sob retenção legal.	Um objeto pode ser excluído após o término do período de retenção, desde que o bucket não esteja sob retenção legal. Os objetos podem ser excluídos automática ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

Tarefas de bloqueio de objeto S3

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

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

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

Administrador de rede

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

Usuário locatário

- Revise as considerações para buckets e objetos com o S3 Object Lock.
- Conforme necessário, entre em contato com o administrador da grade para habilitar a configuração global de bloqueio de objeto do S3 e definir permissões.
- Crie buckets com o S3 Object Lock habilitado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
  - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da rede.
  - Período de retenção padrão: deve ser menor ou igual ao período máximo de retenção definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir a retenção específica do objeto:
  - Modo de retenção. Governança ou conformidade, se permitido pelo administrador da rede.
  - Data de retenção: deve ser menor ou igual ao que é permitido pelo período máximo de retenção definido pelo administrador da grade.

Requisitos para bloqueio de objeto S3

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

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

- Você deve habilitar a configuração global de Bloqueio de Objeto do S3 usando o Grid Manager ou a API de Gerenciamento de Grade antes que qualquer locatário do S3 possa criar um bucket com o Bloqueio de Objeto do S3 habilitado.
- Habilitar a configuração global de Bloqueio de Objeto S3 permite que todas as contas de locatários do S3 criem buckets com o Bloqueio de Objeto S3 habilitado.
- Depois de habilitar a configuração global de Bloqueio de Objeto do S3, você não poderá desabilitá-la.
- Não é possível habilitar o bloqueio de objeto S3 global, a menos que a regra padrão em todas as políticas ativas do ILM seja *compatível* (ou seja, a regra padrão deve estar em conformidade com os requisitos de buckets com o bloqueio de objeto S3 habilitado).

- Quando a configuração global de Bloqueio de Objeto S3 estiver habilitada, você não poderá criar uma nova política de ILM ou ativar uma política de ILM existente, a menos que a regra padrão na política esteja em conformidade. Depois que a configuração global de Bloqueio de Objeto do S3 for habilitada, as páginas de regras e políticas do ILM indicam quais regras do ILM são compatíveis.

Requisitos para regras ILM compatíveis

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

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

Requisitos para políticas de ILM

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

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

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

Requisitos para buckets com bloqueio de objeto S3 habilitado

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

- A replicação do CloudMirror não é suportada para buckets com S3 Object Lock habilitado.

Requisitos para objetos em buckets com bloqueio de objeto S3 habilitado

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

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

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

1. **Ingestão de objetos**

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

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

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

2. **Retenção e exclusão de objetos**

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

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

Informações relacionadas

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

Habilitar bloqueio de objeto S3 globalmente

Se uma conta de locatário do S3 precisar estar em conformidade com requisitos regulatórios ao salvar dados de objeto, você deverá habilitar o Bloqueio de Objeto do S3

para todo o seu sistema StorageGRID . Habilitar a configuração global do S3 Object Lock permite que qualquer usuário locatário do S3 crie e gerencie buckets e objetos com o S3 Object Lock.

Antes de começar

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

Sobre esta tarefa

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

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

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

Passos

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

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

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

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

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

   Quando você seleciona **OK**:

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

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

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

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

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

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

Para resolver esse erro, siga estas etapas:

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

Informações relacionadas

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

Exemplo de regras e políticas do ILM

Exemplo 1: regras e políticas do 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 seus requisitos de proteção e retenção de objetos.

As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

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

Este exemplo de regra ILM copia dados de objeto para pools de armazenamento em dois sites.

Definição de regra	Valor de exemplo
Pools de armazenamento de um único local	Dois pools de armazenamento, cada um contendo sites diferentes, chamados Site 1 e Site 2.
Nome da regra	Duas cópias, dois sites
Tempo de referência	Tempo de ingestão
Posicionamentos	Do Dia 0 até sempre, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

A seção Análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site do StorageGRID será aplicada durante a vigência desta regra.
- Objetos processados por esta regra não serão excluídos pelo ILM.

Regra 2 do ILM, por exemplo 1: Perfil de codificação de apagamento com correspondência de bucket

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

Definição de regra	Valor de exemplo
Pool de armazenamento com vários locais	• Um pool de armazenamento em três locais (locais 1, 2, 3) • Use o esquema de codificação de apagamento 6+3
Nome da regra	Registros financeiros do S3 Bucket
Tempo de referência	Tempo de ingestão
Posicionamentos	Para objetos no bucket do S3 denominados finance-records, crie uma cópia codificada para eliminação no pool especificado pelo perfil de codificação para eliminação. Guarde esta cópia para sempre.

Política ILM, por exemplo 1

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

Uma política de ILM típica para uma grade multisite pode incluir regras de ILM como as seguintes:

- Na ingestão, armazene todos os objetos pertencentes ao bucket S3 denominado `finance-records` em um pool de armazenamento que contém três sites. Use a codificação de eliminação 6+3.

- Se um objeto não corresponder à primeira regra do ILM, use a regra do ILM padrão da política, Duas Cópias, Dois Data Centers, para armazenar uma cópia desse objeto no Site 1 e uma cópia no Site 2.

Informações relacionadas

- "Usar políticas de ILM"
- "Criar políticas de ILM"

Exemplo 2: regras e políticas do ILM 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 filtre por tamanho de objeto para atender aos requisitos de EC recomendados.

As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM, exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo de regra de eliminação do ILM codifica objetos maiores que 1 MB.

A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

Definição de regra	Valor de exemplo
Nome da regra	Objetos somente EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto maior que 1 MB
Posicionamentos	Crie uma cópia codificada para eliminação 2+1 usando três sites

Regra 2 do ILM, por exemplo 2: Duas cópias replicadas

Este exemplo de regra ILM cria duas cópias replicadas e não filtra por tamanho do objeto. Esta regra é a regra padrão para a política. Como a primeira regra filtra todos os objetos maiores que 1 MB, esta regra só se aplica a objetos com 1 MB ou menos.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias replicadas

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Nenhum
Posicionamentos	Do Dia 0 até sempre, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

Política ILM para exemplo 2: Usar EC para objetos maiores que 1 MB

Este exemplo de política de ILM inclui duas regras de ILM:

- A primeira regra de eliminação codifica todos os objetos maiores que 1 MB.
- A segunda regra ILM (padrão) cria duas cópias replicadas. Como objetos maiores que 1 MB foram filtrados pela regra 1, a regra 2 se aplica somente a objetos com 1 MB ou menos.

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

Você pode usar os seguintes exemplos de regras e políticas para garantir que imagens maiores que 1 MB sejam codificadas para eliminação e que duas cópias sejam feitas de imagens menores.

> As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM, exemplo 3: Use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para apagar o código de todos os arquivos de imagem maiores que 1 MB.

> A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

Definição de regra	Valor de exemplo
Nome da regra	Arquivos de imagem EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto maior que 1 MB
Filtros avançados para Chave	• Termina com .jpg • Termina com .png

Definição de regra	Valor de exemplo
Posicionamentos	Crie uma cópia codificada para eliminação 2+1 usando três sites

Como essa regra é configurada como a primeira regra na política, a instrução de posicionamento de codificação de eliminação só se aplica a arquivos .jpg e .png maiores que 1 MB.

Regra 2 do ILM, exemplo 3: Crie 2 cópias replicadas para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que arquivos de imagem menores sejam replicados. Como a primeira regra da política já correspondeu a arquivos de imagem maiores que 1 MB, esta regra se aplica a arquivos de imagem com 1 MB ou menos.

Definição de regra	Valor de exemplo
Nome da regra	2 cópias para arquivos de imagem
Tempo de referência	Tempo de ingestão
Filtros avançados para Chave	• Termina com .jpg • Termina com .png
Posicionamentos	Crie 2 cópias replicadas em dois pools de armazenamento

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

Este exemplo de política de ILM inclui três regras:

- A primeira regra de eliminação codifica todos os arquivos de imagem maiores que 1 MB.
- A segunda regra cria duas cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 1 MB ou menos).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam de imagem).

Exemplo 4: regras e políticas do ILM para objetos versionados do S3

Se você tiver um bucket do S3 com controle de versão habilitado, poderá gerenciar as versões de objetos não atuais incluindo regras na sua política do ILM que usam "Tempo não atual" como tempo de referência.

> Se você especificar um tempo de retenção limitado para objetos, eles serão excluídos permanentemente após o período ser atingido. Certifique-se de entender por quanto tempo os objetos serão retidos.

Como mostra este exemplo, você pode controlar a quantidade de armazenamento usada por objetos versionados usando instruções de posicionamento diferentes para versões de objetos não atuais.

As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Para executar a simulação de política do ILM em uma versão não atual de um objeto, você deve saber o UUID ou CBID da versão do objeto. Para encontrar o UUID e o CBDID, use"pesquisa de metadados de objetos" enquanto o objeto ainda estiver atual.

Informações relacionadas

"Como os objetos são excluídos"

Regra 1 do ILM, por exemplo 4: Guarde três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três sites por 10 anos.

Esta regra se aplica a todos os objetos, independentemente de terem ou não controle de versão.

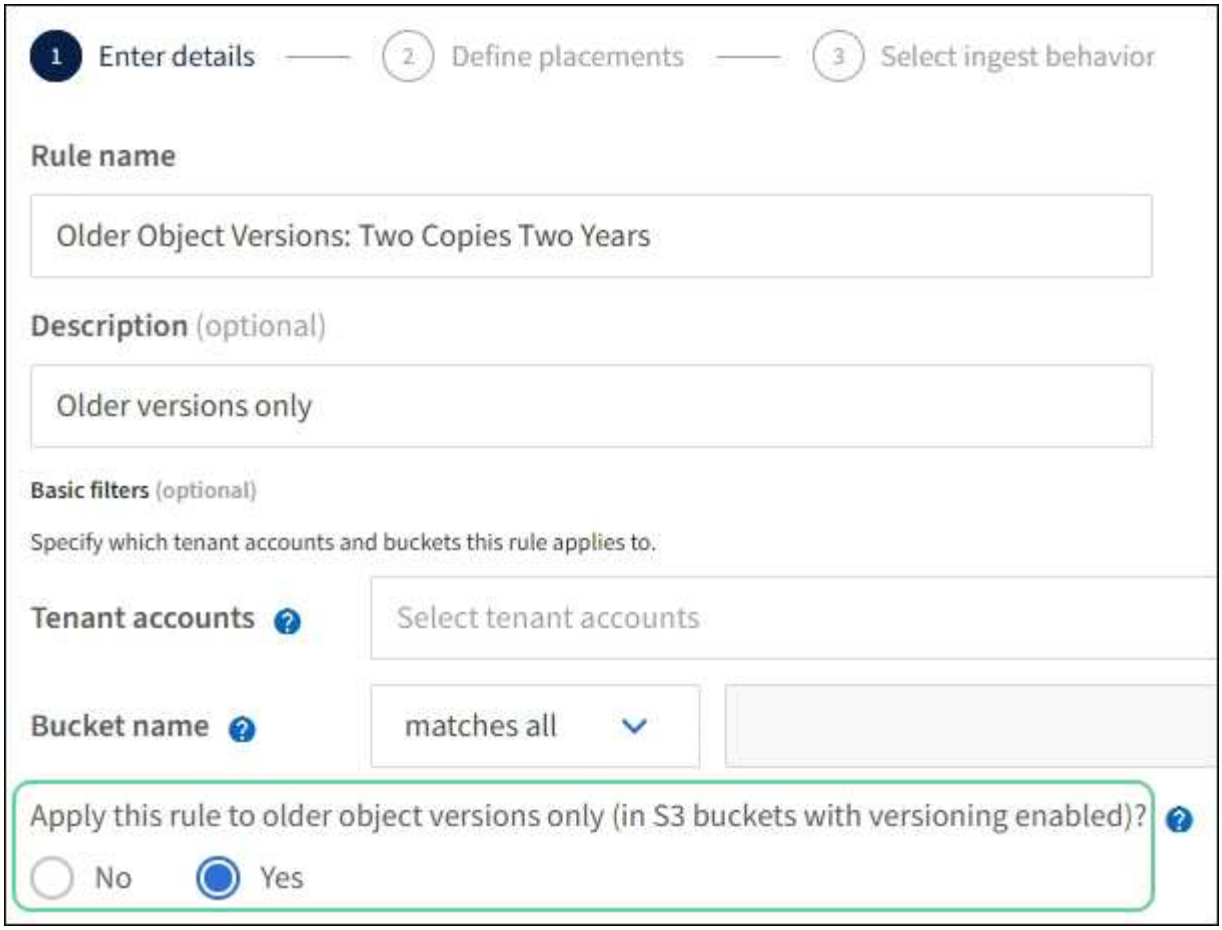
Definição de regra	Valor de exemplo
Pools de armazenamento	Três pools de armazenamento, cada um composto por diferentes data centers, denominados Site 1, Site 2 e Site 3.
Nome da regra	Três cópias dez anos
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no Local 1, uma no Local 2 e uma no Local 3. Ao final de 10 anos, exclua todas as cópias do objeto.

Regra 2 do ILM, 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 versionado do S3 por 2 anos.

Como a regra 1 do ILM se aplica a todas as versões do objeto, você deve criar outra regra para filtrar quaisquer versões não atuais.

Para criar uma regra que usa "Tempo não atual" como tempo de referência, selecione **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" na Etapa 1 (Inserir detalhes) do assistente Criar uma regra do ILM. Quando você seleciona **Sim**, *Horário não atual* é selecionado automaticamente como horário de referência, e você não pode selecionar um horário de referência diferente.



Neste exemplo, apenas duas cópias das versões não atuais são armazenadas, e essas cópias serão armazenadas por dois anos.

Definição de regra	Valor de exemplo
Pools de armazenamento	Dois pools de armazenamento, cada um em diferentes data centers, Site 1 e Site 2.
Nome da regra	Versões não atuais: duas cópias, dois anos
Tempo de referência	Tempo não atual Selecionado automaticamente quando você seleciona **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" no assistente Criar uma regra do ILM.
Posicionamentos	No Dia 0 em relação ao tempo não atual (ou seja, a partir do dia em que a versão do objeto se torna a versão não atual), mantenha duas cópias replicadas das versões não atuais do objeto por 2 anos (730 dias), uma no Site 1 e uma no Site 2. Ao final de 2 anos, exclua as versões não atuais.

Política ILM para o exemplo 4: objetos versionados S3

Se você quiser gerenciar versões mais antigas de um objeto de forma diferente da versão atual, as regras que usam "Tempo não atual" como tempo de referência devem aparecer na política do ILM antes das regras que se aplicam à versão atual do objeto.

Uma política de ILM para objetos versionados do S3 pode incluir regras de ILM como as seguintes:

- Mantenha todas as 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 "Tempo não atual".

- Na ingestão, crie três cópias replicadas e armazene uma cópia em cada um dos três locais. Mantenha cópias da versão atual do objeto por 10 anos.

Ao simular a política de exemplo, você esperaria que os objetos de teste fossem avaliados da seguinte maneira:

- 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 serão removidas da grade).
- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto é armazenada por 10 anos, o processo ILM adiciona um marcador de exclusão como a versão atual do objeto e torna a versão anterior do objeto "não atual". Na próxima vez que ocorrer uma avaliação do ILM, esta versão não atual será correspondida pela primeira regra. Como resultado, a cópia no Site 3 é eliminada e as duas cópias no Site 1 e no Site 2 são armazenadas por mais 2 anos.

Exemplo 5: regras e política do ILM para comportamento de ingestão estrita

Você pode usar um filtro de localização e o comportamento de ingestão Estrito em uma regra para impedir que objetos sejam salvos em um local específico do data center.

Neste exemplo, um inquilino baseado em Paris não quer armazenar alguns objetos fora da UE devido a preocupações regulatórias. Outros objetos, incluindo todos os objetos de outras contas de locatários, podem ser armazenados no data center de Paris ou no data center dos EUA.

> As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Informações relacionadas

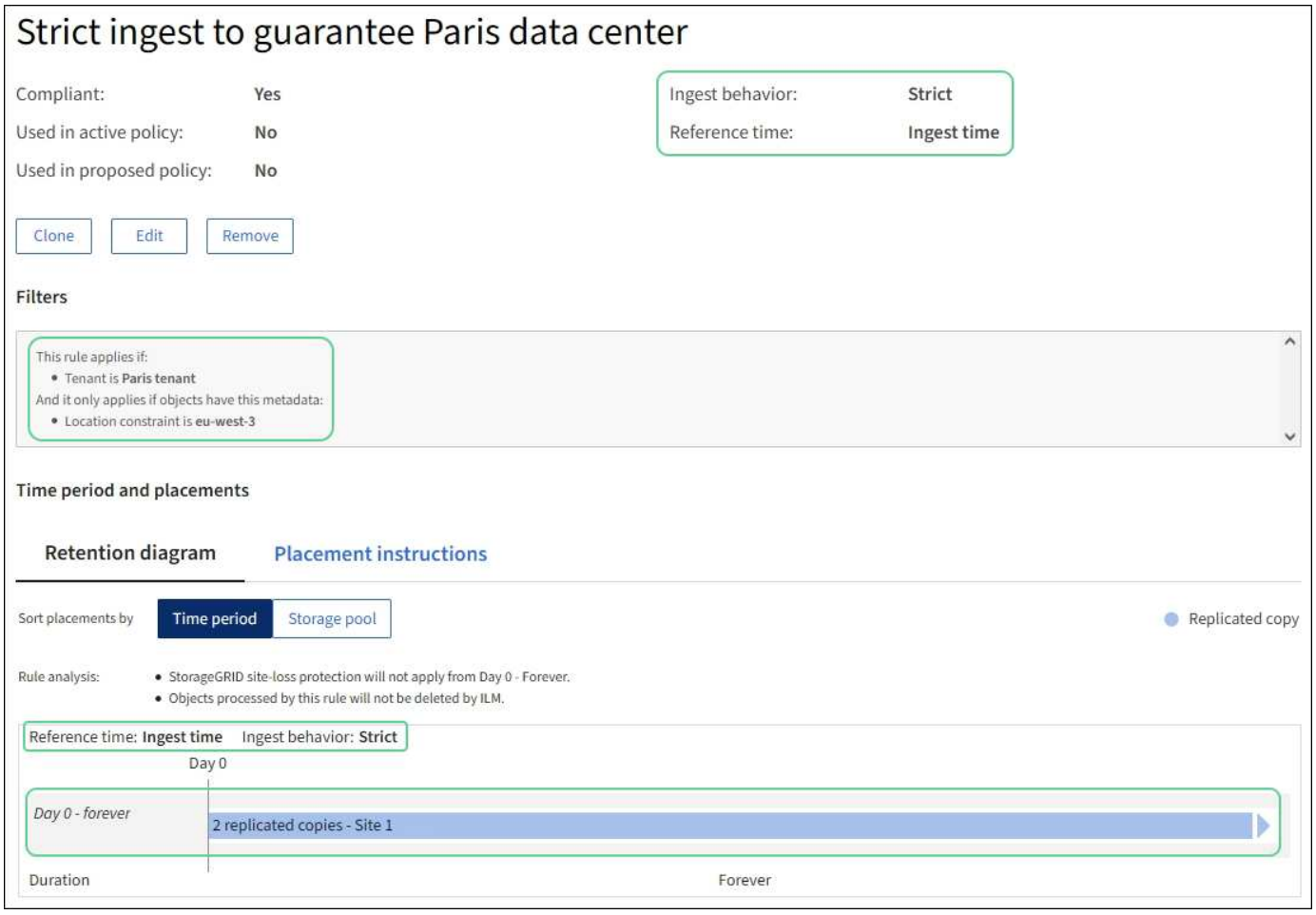
- "Opções de ingestão"
- "Criar regra ILM: selecionar comportamento de ingestão"

Regra 1 do ILM, por exemplo 5: ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra do ILM usa o comportamento de ingestão Strict para garantir que objetos salvos por um locatário baseado em Paris em buckets do S3 com a região definida como eu-west-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra se aplica a objetos que pertencem ao locatário de Paris e que têm a região do bucket S3 definida como eu-west-3 (Paris).

Definição de regra	Valor de exemplo
Conta de inquilino	inquilino de Paris
Filtro avançado	A restrição de localização é igual a eu-west-3
Pools de armazenamento	Sítio 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o centro de dados de Paris
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Estrito. 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 2 do ILM, exemplo 5: ingestão balanceada para outros objetos

Este exemplo de regra de ILM usa o comportamento de ingestão balanceada para fornecer eficiência ideal de ILM para quaisquer objetos não correspondidos pela primeira regra. Duas cópias de todos os objetos correspondentes a esta regra serão armazenadas: uma no centro de dados dos EUA e outra no centro de dados de Paris. Se a regra não puder ser cumprida imediatamente, cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra se aplica a objetos que pertencem a qualquer locatário e qualquer região.

Definição de regra	Valor de exemplo
Conta de inquilino	Ignorar
Filtro avançado	*Não especificado*
Pools de armazenamento	Site 1 (Paris) e Site 2 (EUA)
Nome da regra	2 Cópias 2 Data Centers
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Objetos que correspondem a essa regra são colocados de acordo com as instruções de posicionamento da regra, se possível. Caso contrário, cópias provisórias serão feitas em qualquer local disponível.

Política de ILM para o exemplo 5: Combinando comportamentos de ingestão

O exemplo de política de 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 locatário de Paris e que tenham a região do bucket S3 definida como eu-west-3 (Paris) somente no data center de Paris. Falha na ingestão se o data center de Paris não estiver disponível.
- Armazene todos os outros objetos (incluindo aqueles que pertencem ao locatário de Paris, mas que têm uma região de bucket diferente) no data center dos EUA e no data center de Paris. Faça cópias provisórias em qualquer local disponível se a instrução de posicionamento não puder ser atendida.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte maneira:

- Todos os objetos que pertencem ao locatário de Paris e que têm a região do bucket S3 definida como eu-west-3 são correspondidos pela primeira regra e armazenados no data center de Paris. Como a primeira regra usa ingestão estrita, esses objetos nunca são armazenados no data center dos EUA. Se os nós de armazenamento 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 locatário de Paris e que não têm a região do bucket S3 definida como eu-west-3. Uma cópia de cada objeto é salva em cada centro de dados. No entanto, como a segunda regra usa ingestão balanceada, se um data center não estiver disponível, duas cópias provisórias serão salvas em qualquer local disponível.

Exemplo 6: Alterar uma política de ILM

Se sua proteção de dados precisar ser alterada ou você adicionar novos sites, você poderá criar e ativar uma nova política de ILM.

Antes de alterar uma política, você deve entender como as alterações nos posicionamentos do ILM podem afetar temporariamente o desempenho geral de um sistema StorageGRID .

Neste exemplo, um novo site StorageGRID foi adicionado em uma expansão, e uma nova política de ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro"criar uma política" . Depois, você deve"simular" e então"ativar" a nova política.

> As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Como a alteração de uma política de ILM afeta o desempenho

Ao ativar uma nova política de ILM, o desempenho do seu sistema StorageGRID pode ser temporariamente afetado, especialmente se as instruções de posicionamento 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 quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Para garantir que uma nova política de ILM não afete o posicionamento de objetos replicados e codificados para eliminação existentes, você pode"crie uma regra ILM com um filtro de tempo de ingestão" . Por exemplo, **O tempo de ingestão *é em ou após <data e hora>***, de modo que a nova regra se aplica somente a objetos ingeridos na data e hora especificadas ou após ela.

Os tipos de alterações na política do ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

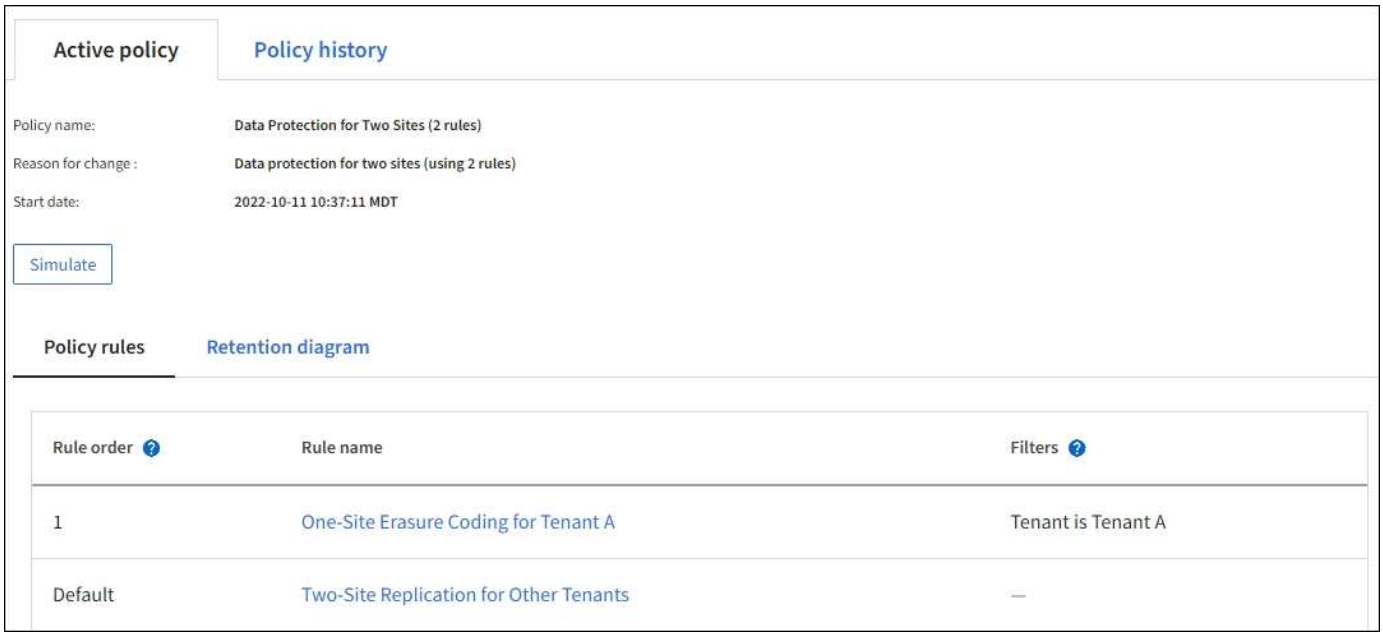
- Aplicar um perfil de codificação de eliminação diferente a objetos codificados por eliminação existentes.

> O StorageGRID considera cada perfil de codificação de eliminação como único e não reutiliza fragmentos de codificação de eliminação 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 para eliminação.
- 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 site remoto.

Política de ILM ativa, por exemplo 6: Proteção de dados em dois sites

Neste exemplo, a política ILM ativa foi projetada inicialmente para um sistema StorageGRID de dois sites e usa duas regras ILM.



Nesta política de ILM, os objetos pertencentes ao Locatário A são protegidos pela codificação de eliminação 2+1 em um único site, enquanto os objetos pertencentes a todos os outros locatários são protegidos em dois sites usando replicação de 2 cópias.

Regra 1: Codificação de eliminação de um site para o Locatário A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de eliminação de um site para o inquilino A
Conta de inquilino	Inquilino A
Pool de armazenamento	Sítio 1
Posicionamentos	Codificação de eliminação 2+1 no Site 1 do dia 0 até sempre

Regra 2: Replicação de dois sites para outros locatários

Definição de regra	Valor de exemplo
Nome da regra	Replicação de dois sites para outros locatários
Conta de inquilino	Ignorar
Pools de armazenamento	Sítio 1 e Sítio 2

Definição de regra	Valor de exemplo
Posicionamentos	Duas cópias replicadas do dia 0 até sempre: uma cópia no Site 1 e uma cópia no Site 2.

Política de ILM, exemplo 6: Proteção de dados em três locais

Neste exemplo, a política ILM está sendo substituída por uma nova política para um sistema StorageGRID de três sites.

Após executar uma expansão para adicionar o novo site, o administrador da grade criou dois novos pools de armazenamento: um pool de armazenamento para o Site 3 e um pool de armazenamento contendo todos os três sites (não o mesmo que o pool de armazenamento padrão Todos os Nós de Armazenamento). Em seguida, o administrador criou duas novas regras de ILM e uma nova política de ILM, projetadas para proteger dados em todos os três sites.

Quando essa nova política de ILM for ativada, os objetos pertencentes ao Locatário A serão protegidos pela codificação de eliminação 2+1 em três sites, enquanto os objetos pertencentes a outros locatários (e objetos menores pertencentes ao Locatário A) serão protegidos em três sites usando replicação de 3 cópias.

Regra 1: Codificação de eliminação de três sites para o Locatário A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de eliminação de três sites para o inquilino A
Conta de inquilino	Inquilino A
Pool de armazenamento	Todos os 3 sites (inclui Site 1, Site 2 e Site 3)
Posicionamentos	Codificação de eliminação 2+1 em todos os 3 sites do dia 0 até sempre

Regra 2: Replicação de três sites para outros inquilinos

Definição de regra	Valor de exemplo
Nome da regra	Replicação de três sites para outros inquilinos
Conta de inquilino	Ignorar
Pools de armazenamento	Sítio 1, Sítio 2 e Sítio 3
Posicionamentos	Três cópias replicadas do dia 0 até sempre: uma cópia no Local 1, uma cópia no Local 2 e uma cópia no Local 3.

Ativando a política ILM, por exemplo 6

Quando você ativa uma nova política 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 de ILM podem causar perda irrecuperável de dados. Revise e simule cuidadosamente a política antes de ativá-la para confirmar se ela funcionará conforme o esperado.

> 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 quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos 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 Locatário A são protegidos usando codificação de eliminação 2+1 no Site 1. Na nova política de ILM, os objetos pertencentes ao Locatário A serão protegidos usando codificação de eliminação 2+1 nos Sites 1, 2 e 3.

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

- Novos objetos ingeridos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Então, cada um dos três fragmentos é armazenado em um local diferente.
- Os objetos existentes pertencentes ao Locatário A são reavaliados durante o processo de verificação do ILM em andamento. Como as instruções de posicionamento do ILM usam um novo perfil de codificação de eliminação, fragmentos inteiramente novos codificados por eliminação são criados e distribuídos para os três locais.

> Os fragmentos 2+1 existentes no Sítio 1 não são reutilizados. O StorageGRID considera cada perfil de codificação de eliminação como único e não reutiliza fragmentos de codificação de eliminação quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política de ILM atualmente ativa para este exemplo, objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de armazenamento nos Sites 1 e 2. Na nova política de ILM, objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de armazenamento nos Sites 1, 2 e 3.

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

- Quando qualquer locatário diferente do Locatário A ingere um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada site.
- Objetos existentes pertencentes a esses outros inquilinos são reavaliados durante o processo de verificação contínua do ILM. Como as cópias de objetos existentes no Site 1 e no Site 2 continuam a atender aos requisitos de replicação da nova regra do ILM, o StorageGRID precisa criar apenas uma nova cópia do objeto para o Site 3.

Impacto no desempenho da ativação desta política

Quando a política ILM neste exemplo for ativada, o desempenho geral deste sistema StorageGRID será temporariamente afetado. Serão necessários níveis de recursos de grade maiores que o normal para criar

novos fragmentos codificados por eliminação para os objetos existentes do Locatário A e novas cópias replicadas no Site 3 para os objetos existentes de outros locatários.

Como resultado da alteração da política de ILM, as solicitações de leitura e gravação do cliente podem apresentar latências temporariamente maiores que o normal. As latências retornarão aos níveis normais depois que as instruções de posicionamento forem totalmente implementadas na grade.

Para evitar problemas de recursos ao ativar uma nova política de ILM, você pode usar o filtro avançado Tempo de ingestão em qualquer regra que possa alterar a localização de um grande número de objetos existentes. Defina o tempo de ingestão como 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 de processamento de objetos após uma alteração na política do ILM.

Exemplo 7: Política ILM compatível para bloqueio de objeto S3

Você pode usar o bucket do S3, as regras do ILM e a política do ILM neste exemplo como ponto de partida ao definir uma política do ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o Bloqueio de Objeto do S3 habilitado.

Se você usou o recurso de conformidade legado em versões anteriores do StorageGRID , também pode usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de conformidade legado habilitado.

As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Informações relacionadas

- "Gerenciar objetos com o S3 Object Lock"
- "Criar uma política de ILM"

Exemplo de bucket e objetos para bloqueio de objeto S3

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Tenant Manager para criar um bucket com o S3 Object Lock habilitado para armazenar registros bancários críticos.

Definição de balde	Valor de exemplo
Nome da conta do inquilino	Banco do ABC
Nome do balde	registros bancários
Região do balde	us-east-1 (padrão)

Cada objeto e versão de objeto que for adicionado ao bucket de registros bancários usará os seguintes valores para `retain-until-date` e `legal hold` configurações.

Configuração para cada objeto	Valor de exemplo
`retain-until-date`	"2030-12-30T23:59:59Z" (30 de dezembro de 2030) Cada versão do objeto tem sua própria `retain-until-date` contexto. Esta configuração pode ser aumentada, mas não diminuída.
`legal hold`	"OFF" (Não em vigor) Uma retenção legal pode ser colocada ou suspensa em qualquer versão do objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob retenção legal, o objeto não poderá ser excluído, mesmo que `retain-until-date` foi alcançado.

Exemplo de regra 1 do ILM para bloqueio de objeto S3: perfil de codificação de eliminação com correspondência de bucket

Este exemplo de regra do ILM se aplica somente à conta de locatário do S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa codificação de eliminação para armazenar o objeto em nós de armazenamento em três locais de data center usando um perfil de codificação de eliminação 6+3. Esta regra atende aos requisitos de buckets com o S3 Object Lock habilitado: uma cópia é mantida nos nós de armazenamento do dia 0 até sempre, usando o tempo de ingestão como tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra de conformidade: Objetos EC no Bucket de registros bancários - Banco do ABC
Conta de inquilino	Banco do ABC
Nome do balde	`bank-records`
Filtro avançado	Tamanho do objeto (MB) maior que 1 **Observação:** Este filtro garante que a codificação de eliminação não seja usada para objetos de 1 MB ou menores.

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Posicionamentos	Desde o dia 0, armazene para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada para eliminação em nós de armazenamento em três locais de data center • Utiliza esquema de codificação de apagamento 6+3

Exemplo de regra 2 do ILM para bloqueio de objeto S3: regra não compatível

Este exemplo de regra ILM armazena inicialmente duas cópias de objetos replicadas em nós de armazenamento. Após um ano, ele armazena uma cópia em um pool de armazenamento em nuvem para sempre. Como essa regra usa um pool de armazenamento em nuvem, ela não é compatível e não se aplicará aos objetos em buckets com o bloqueio de objeto do S3 habilitado.

Definição de regra	Valor de exemplo
Nome da regra	Regra não compatível: usar pool de armazenamento em nuvem
Contas de inquilinos	Não especificado
Nome do balde	Não especificado, mas só será aplicado a buckets que não tenham o S3 Object Lock (ou o recurso de conformidade legado) habilitado.
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Posicionamentos	• No Dia 0, mantenha duas cópias replicadas nos Nós de Armazenamento no Data Center 1 e no Data Center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um pool de armazenamento em nuvem para sempre

Exemplo de regra 3 do ILM para bloqueio de objeto S3: regra padrão

Este exemplo de regra ILM copia dados de objeto para pools de armazenamento em dois data centers. Esta regra compatível foi criada para ser a regra padrão na política do ILM. Ele não inclui nenhum filtro, não usa o tempo de referência Não Atual e atende aos requisitos de buckets com Bloqueio de Objeto S3 habilitado: duas cópias de objeto são mantidas em Nós de Armazenamento do dia 0 até sempre, usando Ingestão como o tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra padrão compatível: Duas cópias, dois data centers
Conta de inquilino	Não especificado
Nome do balde	Não especificado
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão

Definição de regra	Valor de exemplo
Posicionamentos	Do Dia 0 até sempre, mantenha duas cópias replicadas: uma nos Nós de Armazenamento no Data Center 1 e uma nos Nós de Armazenamento no Data Center 2.

Exemplo de política de ILM compatível para bloqueio de objeto S3

Para criar uma política de ILM que proteja efetivamente todos os objetos no seu sistema, incluindo aqueles em buckets com o S3 Object Lock habilitado, você deve selecionar regras de ILM que atendam aos requisitos de armazenamento para todos os objetos. Então, você deve simular e ativar a política.

Adicionar regras à política

Neste exemplo, a política de ILM inclui três regras de ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de eliminação para proteger objetos maiores que 1 MB em um bucket específico com o S3 Object Lock habilitado. Os objetos são armazenados em nós de armazenamento do dia 0 até sempre.
2. Uma regra não compatível que cria duas cópias de objetos replicadas em nós de armazenamento por um ano e depois move uma cópia de objeto para um pool de armazenamento em nuvem para sempre. Esta regra não se aplica a buckets com o S3 Object Lock habilitado porque ele usa um Cloud Storage Pool.
3. A regra padrão compatível que cria duas cópias de objetos replicadas em nós de armazenamento do dia 0 até sempre.

Simule a política

Depois de adicionar regras à sua política, escolher uma regra padrão compatível e organizar as outras regras, você deve simular a política testando objetos do bucket com o Bloqueio de Objeto S3 habilitado e de outros buckets. Por exemplo, ao simular a política de exemplo, você esperaria que os objetos de teste fossem avaliados da seguinte maneira:

- A primeira regra corresponderá somente a objetos de teste maiores que 1 MB nos registros bancários do bucket 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 locatários.
- A regra padrão corresponderá a estes objetos:
  - Objetos de 1 MB ou menores nos registros bancários do bucket para o locatário do Bank of ABC.
  - Objetos em qualquer outro bucket que tenha o Bloqueio de Objeto do S3 habilitado para todas as outras contas de locatário.

Ativar a política

Quando estiver completamente satisfeito de que a nova política protege os dados do objeto conforme o esperado, você poderá ativá-la.

Exemplo 8: Prioridades para o ciclo de vida do bucket S3 e política de ILM

Dependendo da configuração do seu ciclo de vida, os objetos seguem as configurações de retenção do ciclo de vida do bucket do S3 ou de uma política do ILM.

Exemplo de ciclo de vida de bucket tendo prioridade sobre política de ILM

Política de ILM

- Regra baseada em referência de tempo não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, mantenha X cópias por 50 dias

Ciclo de vida do balde

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket do prefixo "docs/".
  - Após 100 dias, um marcador de exclusão é criado e "docs/text" se torna não atual.
  - Após 5 dias, um total de 105 dias desde a ingestão, "docs/text" é excluído.
  - Após 95 dias, um total de 200 dias desde a ingestão e 100 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.
- Um objeto chamado "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção do ILM.
  - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" deixa de ser atual.
  - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.
  - Após 30 dias, um total de 100 dias desde a ingestão e 50 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.

Exemplo de ciclo de vida de bucket mantendo implicitamente para sempre

Política de ILM

- Regra baseada em referência de tempo não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, mantenha X cópias por 50 dias

Ciclo de vida do balde

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket do prefixo "docs/".

  O `Expiration` a ação se aplica somente a marcadores de exclusão expirados, o que implica manter todo o resto para sempre (começando com "docs/").

  Os marcadores de exclusão que começam com "docs/" são removidos quando expiram.

- Um objeto chamado "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção do ILM.
  - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" deixa de ser atual.
  - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.

- Após 30 dias, um total de 100 dias desde a ingestão e 50 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.

Exemplo de uso do ciclo de vida do bucket para duplicar o ILM e limpar marcadores de exclusão expirados

Política de ILM

- Regra baseada em referência de tempo não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, manter X cópias para sempre

Ciclo de vida do balde

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- A política ILM é duplicada no ciclo de vida do bucket.
  - A regra "para sempre" da política ILM foi projetada para remover objetos manualmente e limpar versões não atuais após 20 dias. Consequentemente, a regra de tempo de ingestão manterá os marcadores de exclusão expirados para sempre.
  - O ciclo de vida do bucket duplica o comportamento da política ILM ao adicionar `"ExpiredObjectDeleteMarker": true` , que remove marcadores de exclusão quando eles expiram
- Um objeto é ingerido. Nenhum filtro significa que o ciclo de vida do bucket se aplica a todos os objetos e substitui as configurações de retenção do ILM.
  - Quando um locatário emite uma solicitação de exclusão de objeto, um marcador de exclusão é criado e o objeto se torna não atual.
  - Após 20 dias, o objeto não atual é excluído e o marcador de exclusão expira.
  - Pouco depois, o marcador de exclusão expirado é excluído.

Informações sobre direitos autorais

Informações sobre marcas comerciais