



Gerencie objetos com ILM

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/storagegrid-120/ilm/index.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Índice

Gerencie objetos com ILM	1
Gerencie objetos com ILM no StorageGRID	1
Sobre estas instruções	1
Saiba mais	1
ILM e ciclo de vida de objetos	1
Como o ILM opera ao longo do ciclo de vida de um objeto no StorageGRID	1
Como os objetos são ingeridos	3
Como os objetos são armazenados (replicação ou codificação de apagamento)	8
Como StorageGRID determina a retenção de objetos	19
Como StorageGRID exclui objetos	21
Crie e atribua níveis de storage no StorageGRID	24
Utilize pools de storage	27
Saiba mais sobre pool de storage no StorageGRID	27
Diretrizes de configuração do pool de storage no StorageGRID	28
Proteção contra perda de sites com pools de storage no StorageGRID	29
Crie um pool de storage no StorageGRID	31
Veja os detalhes do pool de storage no StorageGRID	33
Editar um pool de storage no StorageGRID	34
Remover um pool de storage no StorageGRID	35
Use Cloud Storage Pools	35
Saiba mais sobre Cloud Storage Pools no StorageGRID	35
Ciclo de vida de um objeto de pool de storage em nuvem no StorageGRID	37
Casos de uso do Cloud Storage Pool no StorageGRID	39
Requisitos e limites do Cloud Storage Pool no StorageGRID	40
Pools de armazenamento em nuvem e CloudMirror replication no StorageGRID	43
Criar um Cloud Storage Pool no StorageGRID	45
Veja os detalhes do Cloud Storage Pool no StorageGRID	48
Editar um Cloud Storage Pool no StorageGRID	49
Remover um Cloud Storage Pool no StorageGRID	50
Solucione problemas de Cloud Storage Pools no StorageGRID	51
Gerencie perfis de codificação de apagamento no StorageGRID	55
Veja os detalhes do perfil de codificação de apagamento	55
Renomear um perfil de codificação de apagamento	55
Desativar um perfil de codificação de apagamento	55
Configure regiões S3 para StorageGRID	58
Criar regra ILM	60
Saiba mais sobre as regras ILM no StorageGRID	60
Acesse o assistente Criar uma regra ILM no StorageGRID	64
Insira detalhes e filtros para uma regra ILM do StorageGRID	65
Defina as instruções de posicionamento para uma regra ILM do StorageGRID	69
Use tempo de acesso nas regras do StorageGRID ILM	73
Selecione o comportamento de ingestão para uma regra ILM do StorageGRID	74
Crie uma regra ILM padrão no StorageGRID	75

Gerenciar políticas ILM	77
Saiba mais sobre as políticas ILM no StorageGRID	77
Crie políticas ILM no StorageGRID	81
Exemplo de simulações de políticas ILM no StorageGRID	87
Gerencie tags de política ILM no StorageGRID	90
Verifique uma política ILM com pesquisa de metadados de objeto no StorageGRID	91
Trabalhe com políticas ILM e regras ILM no StorageGRID	93
Ver políticas do ILM	94
Editar uma política ILM	94
Clonar uma política ILM	94
Remover uma política ILM	95
Veja os detalhes da regra ILM	95
Clonar uma regra ILM	95
Editar uma regra ILM	96
Remover uma regra ILM	96
Visualizar métricas de ILM	97
Use o Bloqueio de Objeto S3	98
Como o S3 Object Lock protege objetos no StorageGRID	98
Fluxo de trabalho do S3 Object Lock no StorageGRID	101
Requisitos do S3 Object Lock no StorageGRID	101
Ativar o S3 Object Lock globalmente no StorageGRID	104
Resolva erros de consistência ao atualizar S3 Object Lock ou configurações de Compliance legadas no StorageGRID	105
Exemplos de regras e políticas de ILM	106
Regras e políticas do ILM para proteção básica de objetos e retenção no StorageGRID	106
Regras e política de ILM para filtragem de tamanho de objetos EC no StorageGRID	109
Regras e política de ILM para proteger arquivos de imagem no StorageGRID	110
Regras e políticas de ILM para versões não atuais de objetos S3 no StorageGRID	112
Regras e política de ILM para comportamento de ingestão estrito no StorageGRID	115
Como a alteração de uma política ILM afeta o desempenho do StorageGRID	117
Política ILM compatível para S3 Object Lock no StorageGRID	121
Como o ciclo de vida do bucket S3 e a política ILM interagem no StorageGRID	125

Gerencie objetos com ILM

Gerencie objetos com ILM no StorageGRID

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 dos 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 compreender seus requisitos operacionais, a topologia do seu sistema StorageGRID, suas necessidades de proteção de objetos e os tipos de storage disponíveis. Depois, você deve determinar como deseja que diferentes tipos de objetos sejam copiados, distribuídos e armazenados.

Use estas instruções para:

- Saiba mais sobre StorageGRID ILM, incluindo ["Como o ILM opera ao longo da vida útil de um objeto"](#).
- Aprenda como configurar ["pools de storage"](#), ["Pools de storage em nuvem"](#) e ["Regras do ILM"](#).
- Aprenda como ["criar, simular e ativar uma política ILM"](#) proteger os dados de objetos em um ou mais sites.
- Aprenda como ["Gerencie objetos com S3 Object Lock"](#), o que ajuda a garantir que objetos em buckets específicos do S3 não sejam excluídos ou sobrescritos por um período de tempo determinado.

Saiba mais

Para saber mais, confira estes vídeos:

[Visão geral das regras do ILM](#)

[Visão geral das políticas do ILM](#)

ILM e ciclo de vida de objetos

Como o ILM opera ao longo do ciclo de vida de um objeto no StorageGRID

Compreender como StorageGRID usa o ILM para gerenciar objetos em cada etapa do seu ciclo de vida 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" para o cliente. Os dados do objeto são protegidos durante a ingestão, seja aplicando instruções de ILM imediatamente (posicionamento síncrono) ou criando cópias intermediárias e aplicando o ILM posteriormente (confirmação dupla), dependendo de como os requisitos de ILM foram especificados.
- **Gerenciamento de cópias:** Após criar o número e o tipo de cópias de objetos especificados nas instruções de posicionamento do ILM, StorageGRID gerencia os locais dos objetos e os protege contra perda.
 - **Verificação e avaliação do ILM:** StorageGRID verifica continuamente a lista de objetos armazenados

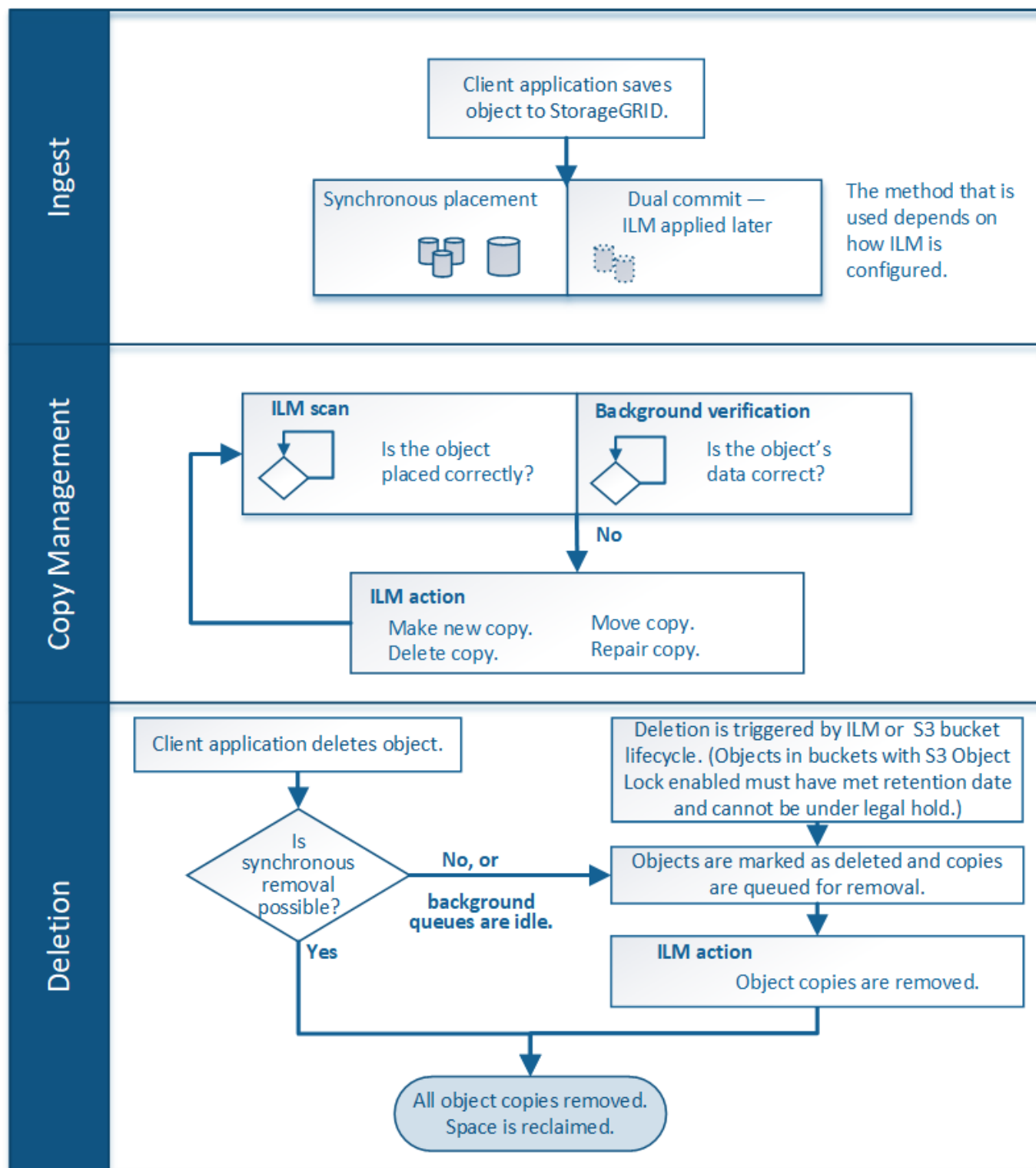
na grid e verifica se as cópias atuais atendem aos requisitos do ILM. Quando são necessários diferentes tipos, números ou locais de cópias de objetos, StorageGRID cria, exclui ou move cópias conforme necessário.

- **Verificação em segundo plano:** StorageGRID realiza verificações contínuas em segundo plano para verificar a integridade dos dados do objeto. Se um problema for encontrado, StorageGRID cria automaticamente uma nova cópia do objeto ou um fragmento de objeto com codificação de apagamento em um local que atenda aos requisitos atuais do ILM. Consulte ["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 feita por um cliente, ou como resultado da exclusão pelo ILM ou da exclusão causada pela expiração do ciclo de vida do bucket S3.



Os objetos em um bucket com o S3 Object Lock ativado não podem ser excluídos se estiverem sob guarda legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida.

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



Como os objetos são ingeridos

Opções de ingestão de ILM no StorageGRID

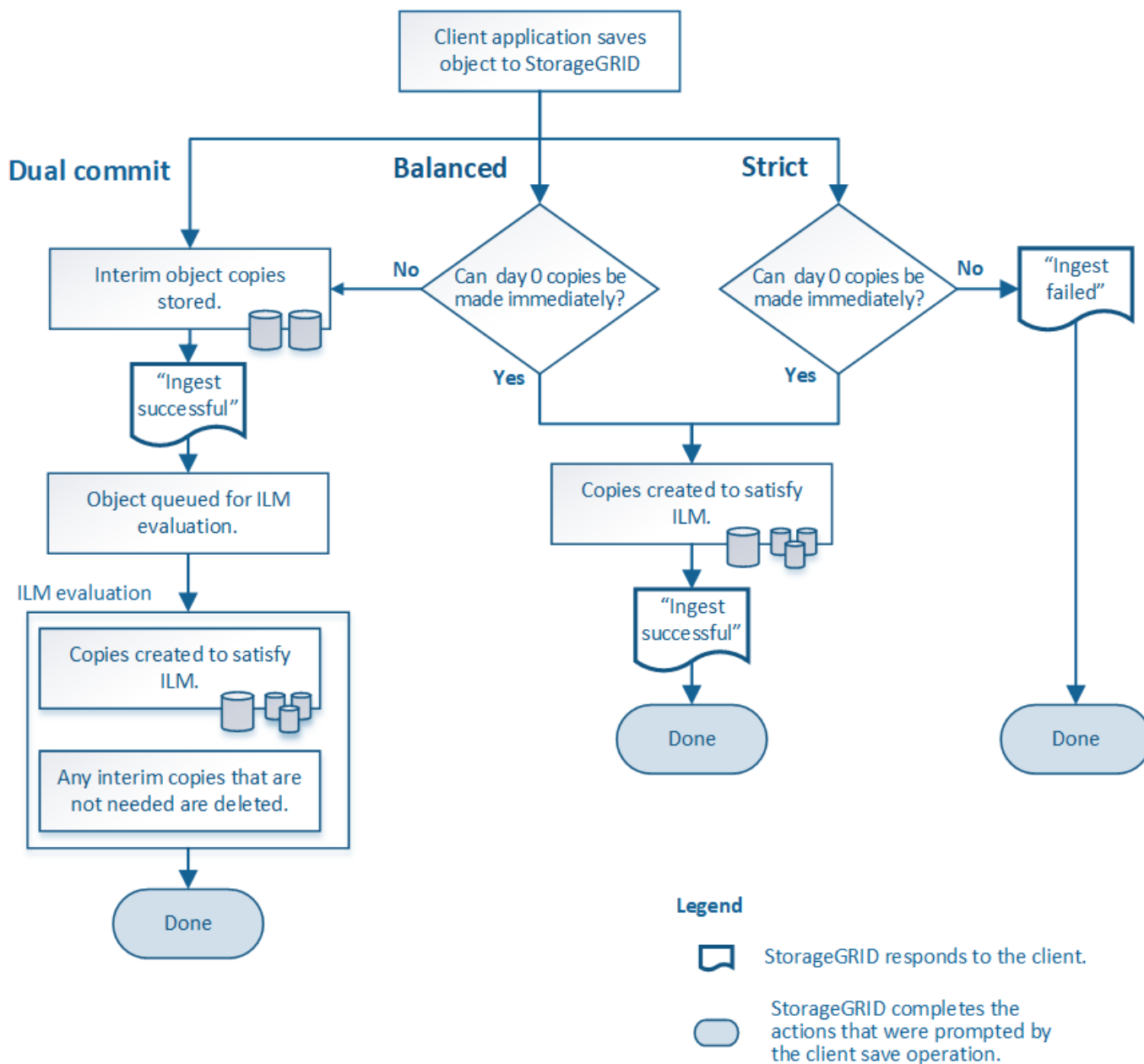
Ao criar uma regra ILM, você especifica uma das três opções para proteger objetos na ingestão: dual commit, strict ou balanced.

Dependendo da sua escolha, StorageGRID cria cópias provisórias e enfileira os objetos para avaliação do ILM

posteriormente, ou utiliza o posicionamento síncrono e cria cópias imediatamente para atender aos requisitos do ILM.

Fluxograma das 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 ingest.



Commit duplo

Ao selecionar a opção Dual commit, StorageGRID cria imediatamente cópias provisórias do objeto em dois nós de armazenamento diferentes e retorna uma mensagem de "ingest successful" para o cliente. O objeto é enfileirado para avaliação do ILM e as cópias que atendem às instruções de posicionamento da regra são criadas posteriormente. Se a política do ILM não puder ser processada imediatamente após o dual commit, a proteção contra perda de site pode levar algum tempo para ser alcançada.

Utilize a opção de confirmação dupla em qualquer um destes casos:

- Você está usando regras ILM em vários sites e a latência de ingestão do cliente é sua principal consideração. Ao usar o Dual commit, você deve garantir que seu grid possa executar o trabalho adicional de criar e remover as cópias de dual commit caso elas não atendam ao ILM. Especificamente:
 - A carga na grid deve ser suficientemente baixa para evitar um backlog de ILM.
 - A rede deve ter recursos de hardware excedentes (IOPS, CPU, memória, largura de banda, e assim por diante).
- Você está usando regras ILM em vários sites e a conexão WAN entre os sites geralmente apresenta alta latência ou largura de banda limitada. Nesse cenário, usar a opção Dual commit pode ajudar a evitar timeouts do cliente. Antes de escolher a opção Dual commit, você deve testar o aplicativo cliente com cargas de trabalho realistas.

Equilibrado (padrão)

Ao selecionar a opção Balanceada, StorageGRID também usa o posicionamento síncrono na ingestão e cria imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção Estrita, se StorageGRID não puder criar imediatamente todas as cópias, ele usa o Dual commit. Se a política ILM usar posicionamentos em vários sites e a proteção imediata contra perda de site não puder ser alcançada, o alerta **ILM placement unachievable** será acionado.

Use a opção Balanced para obter a melhor combinação de proteção de dados, desempenho do grid e sucesso na ingestão. Balanced é a opção padrão no assistente Criar regra ILM.

Estrito

Ao selecionar a opção Estrita, StorageGRID usa o posicionamento síncrono na ingestão e cria imediatamente todas as cópias de objetos especificadas nas instruções de posicionamento da regra. A ingestão falha se StorageGRID não conseguir criar todas as cópias, por exemplo, porque um local de storage necessário está temporariamente indisponível. O cliente deve tentar a operação novamente.

Use a opção Estrita se você tiver um requisito operacional ou regulamentar para armazenar objetos imediatamente apenas nos locais definidos na regra ILM. Por exemplo, para atender a um requisito regulamentar, você pode precisar usar a opção Estrita e um filtro avançado de Restrição de Localização para garantir que os objetos nunca sejam armazenados em determinados data centers.

Consulte ["Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"](#).

Vantagens, desvantagens e limitações das opções de ingest de ILM no StorageGRID

Compreender as vantagens e desvantagens de cada uma das três opções para proteger os dados na ingestão (Balanced, Strict ou Dual commit) pode ajudar você a decidir qual selecionar para uma regra ILM.

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

Vantagens das opções Equilibrada e Rigorosa

Em comparação com o Dual commit, que cria cópias provisórias durante a ingestão, as duas opções de posicionamento síncrono podem oferecer as seguintes vantagens:

- **Maior segurança de dados:** Os dados do objeto são protegidos imediatamente, 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 storage. O commit duplo só pode proteger contra a perda de uma única cópia local.

- **Operação de grid mais eficiente:** Cada objeto é processado apenas uma vez, no momento da ingestão. Como o sistema StorageGRID não precisa rastrear ou excluir cópias intermediárias, há menos carga de processamento e menos espaço de banco de dados consumido.
- **(Balanced) Recomendado:** A opção Balanced oferece eficiência ideal do ILM. Recomenda-se o uso da opção Balanced, a menos que seja necessário um comportamento de ingestão estrito ou que o grid atenda a todos os critérios para usar o Dual commit.
- **Certeza (estrita) sobre a localização dos objetos:** A opção Strict garante que os objetos sejam armazenados imediatamente de acordo com as instruções de posicionamento na regra ILM.

Desvantagens das opções Equilibrada e Rigorosa

Em comparação com o Dual commit, as opções Balanced e Strict apresentam algumas desvantagens:

- **Ingestão mais demorada por parte do cliente:** A latência de ingestão por parte do cliente pode ser maior. Ao usar as opções Balanced ou Strict, uma mensagem de "ingestão bem-sucedida" não é retornada ao cliente até que todos os fragmentos de codificação de apagamento ou cópias replicadas sejam criados e armazenados. No entanto, os dados do objeto provavelmente chegarão ao seu destino final muito mais rapidamente.
- **(Estrito) Taxas mais altas de falha na ingestão:** Com a opção Estrito, a ingestão falha sempre que StorageGRID não consegue fazer imediatamente todas as cópias especificadas na regra ILM. Você pode observar altas taxas de falha na ingestão se um local de storage necessário estiver temporariamente offline ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(Estrito) Em algumas circunstâncias, o posicionamento dos uploads multipartes no S3 pode não ser o esperado:** Com o modo Estrito, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. No entanto, em um upload multipartes no S3, o ILM é avaliado para cada parte do objeto à medida que é ingerida e para o objeto como um todo quando o upload multipartes é concluído. Nas seguintes circunstâncias, isso pode resultar em posicionamentos diferentes do que você espera:
 - **Se o ILM for alterado durante um upload multipart do S3:** Como cada parte é posicionada de acordo com a regra ativa no momento da ingestão, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Nesses casos, a ingestão do objeto não falha. Em vez disso, qualquer parte que não esteja posicionada corretamente é enfileirada 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 parte, StorageGRID filtra pelo tamanho da parte, 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 com 10 GB ou mais sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenada no DC2. Quando o ILM é avaliado para o objeto, todas as partes do objeto são movidas para o DC1.
- **(Estrito) A ingestão não falha quando as tags ou metadados são atualizados e os novos posicionamentos necessários não podem ser feitos:** Com o modo Estrito, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. No entanto, ao atualizar metadados ou tags de um objeto já armazenado na grid, o objeto não é reingerido. Isso significa que quaisquer alterações no posicionamento do objeto acionadas pela atualização não são feitas imediatamente. As 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 **Balanced** e **Strict**

As opções **Equilibrado** ou **Rigorous** não podem ser usadas para regras ILM que tenham alguma destas instruções de posicionamento:

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

Essas restrições existem porque StorageGRID não consegue fazer cópias síncronas para um Cloud Storage Pool, e um horário de criação definido pelo usuário pode ser resolvido para o presente.

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

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

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

Segue um breve resumo dos valores de consistência disponíveis no StorageGRID:

- **Todos:** Todos os nós recebem metadados de objeto imediatamente ou a solicitação falhará.
- **Strong-global:** Garante a consistência de leitura após gravação para todas as solicitações do cliente em todos os sites. Quando a semântica de Quorum está configurada, os seguintes comportamentos se aplicam:
 - Permite tolerância a falha do local para solicitações de clientes quando as grades têm três ou mais sites. Grades com dois sites não terão tolerância a falha do local.
 - As seguintes operações do S3 não serão bem-sucedidas com um site inativo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Se necessário, você pode ["configurar a semântica de quorum do StorageGRID para consistência global forte"](#).

- **Strong-site:** os metadados do objeto são distribuídos imediatamente para outros nós no site. Garante a consistência de leitura após gravação para todas as solicitações do cliente dentro de um site.
- **Leitura após nova gravação:** Oferece 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:** Oferece consistência eventual tanto para novos objetos quanto para atualizações de objetos. Para buckets do S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que são lidos raramente ou para operações HEAD ou GET em chaves que não existem). Não é compatível com buckets do S3 FabricPool.



Antes de selecionar um valor de consistência, "[Leia a descrição completa de consistência](#)". Você deve entender os benefícios e as limitações antes de alterar o valor padrão.

Exemplo de como as regras de consistência e ILM podem interagir

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

- **Regra ILM:** Crie três cópias do objeto, uma no local e uma em cada local remoto. Use o comportamento de ingestão estrito.
- **Consistência:** Global forte (os metadados do objeto são distribuídos imediatamente para vários sites).

Quando um cliente armazena um objeto na grid, StorageGRID cria as três cópias do objeto e distribui os metadados para vários sites antes de retornar sucesso ao cliente.

O objeto fica totalmente protegido contra perda no momento em que a mensagem de ingestão bem-sucedida é recebida. Por exemplo, se o local remoto for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão nos locais remotos. O objeto poderá ser recuperado integralmente dos outros locais.

Se, em vez disso, você usasse a mesma regra ILM e a consistência forte do site, o cliente poderia receber uma mensagem de sucesso após os dados do objeto serem replicados para os locais remotos, 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 local remoto for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre as regras de consistência e as regras de ILM pode ser complexa. Entre em contato com a NetApp se você precisar de assistência.

Informações relacionadas

["Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"](#)

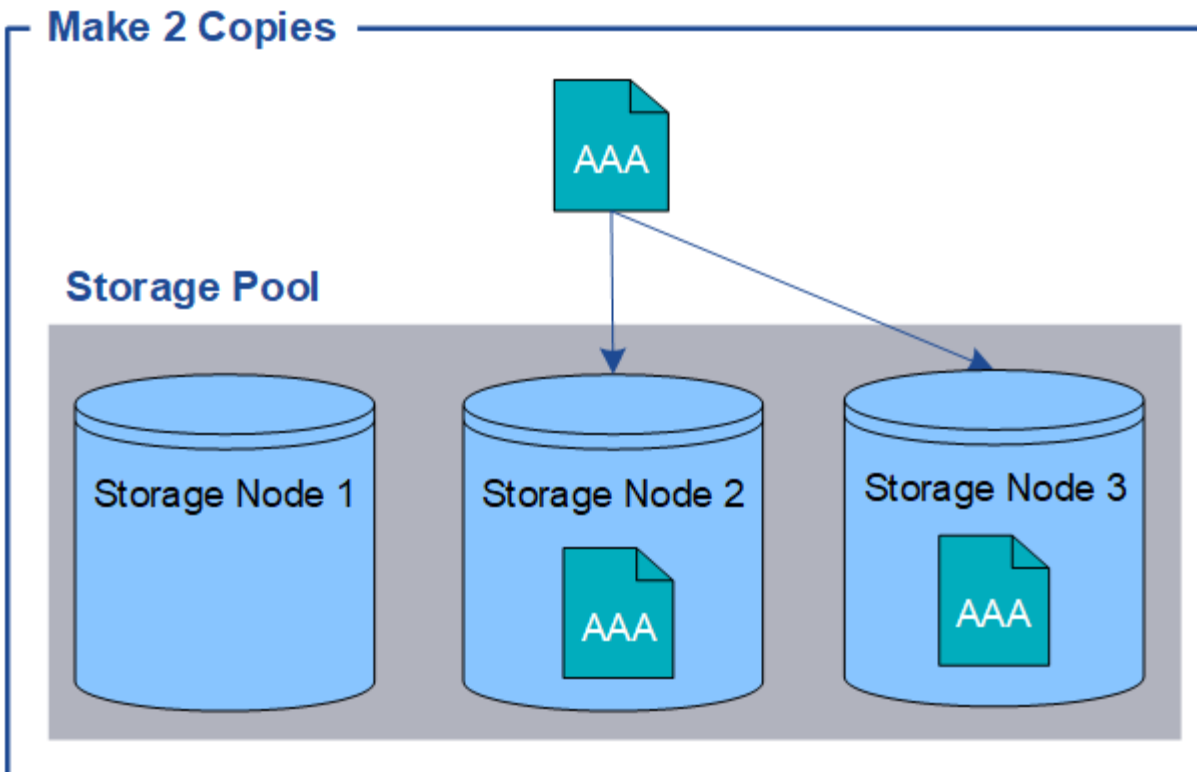
Como os objetos são armazenados (replicação ou codificação de apagamento)

Saiba mais sobre replicação no StorageGRID

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

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

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



Quando StorageGRID encontra objetos que correspondem a esta regra, ele cria duas cópias do objeto, colocando cada cópia em um Storage Node diferente no pool de storage. As duas cópias podem ser colocadas em quaisquer dois dos três Storage Nodes disponíveis. Neste caso, a regra colocou cópias do objeto nos Storage Nodes 2 e 3. Como existem duas cópias, o objeto pode ser recuperado se algum dos nós no pool de storage falhar.



StorageGRID só pode armazenar uma cópia replicada de um objeto em qualquer Storage Node. Se sua grid incluir três Storage Nodes e você criar uma regra ILM de 4 cópias, apenas três cópias serão criadas, uma cópia para cada Storage Node. 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 storage"](#)
- ["Habilite a proteção contra perda de site usando replicação e codificação de apagamento"](#)

Riscos da replicação de cópia única no StorageGRID

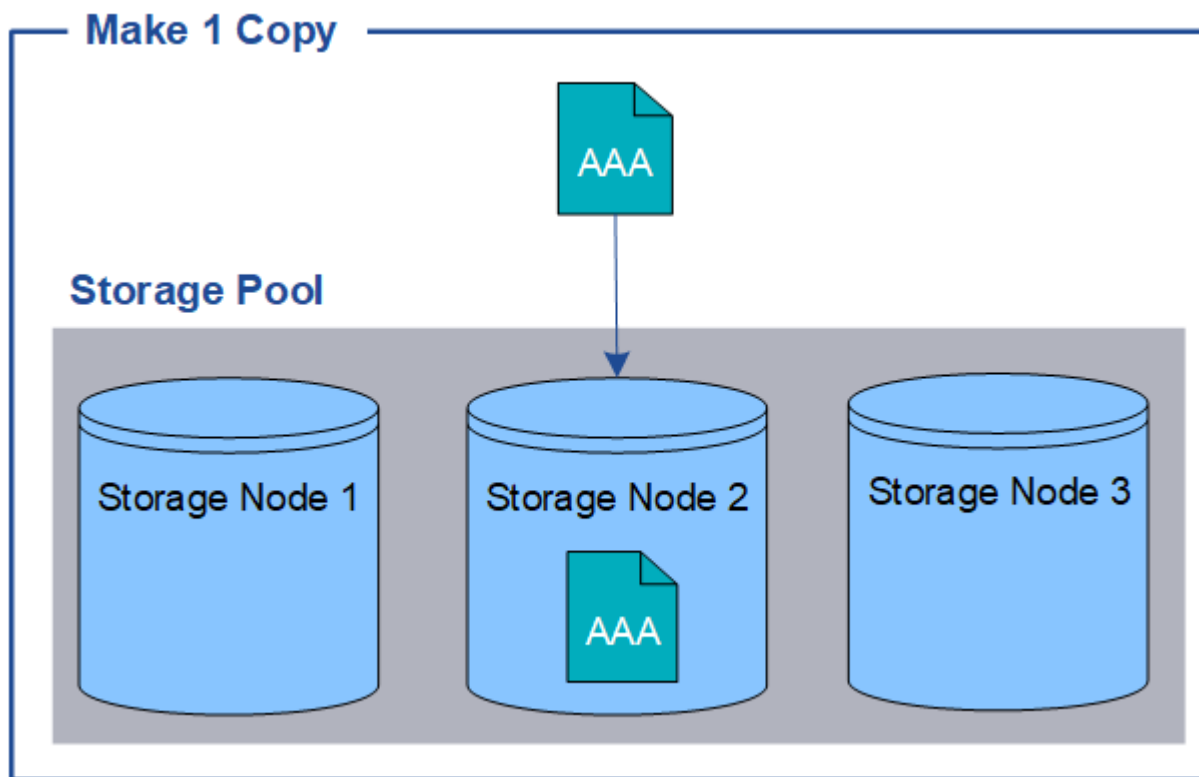
Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de posicionamento.



Não utilize uma regra 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 Storage Node falhar ou apresentar um erro significativo. Você também perderá temporariamente o acesso ao objeto durante procedimentos de manutenção, como upgrades.

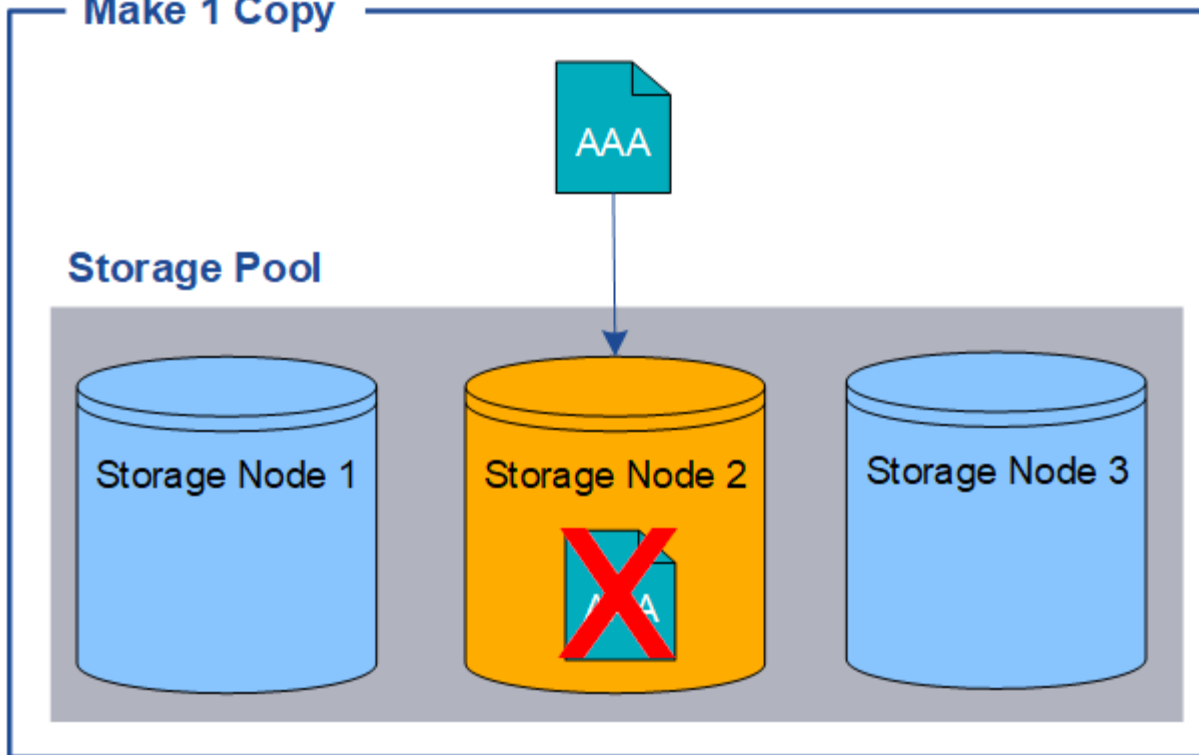
No exemplo a seguir, a regra ILM "Make 1 Copy" especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contenha três Storage Nodes. Quando um objeto que corresponde a

essa regra é ingerido, StorageGRID coloca uma única cópia em apenas um Storage Node.

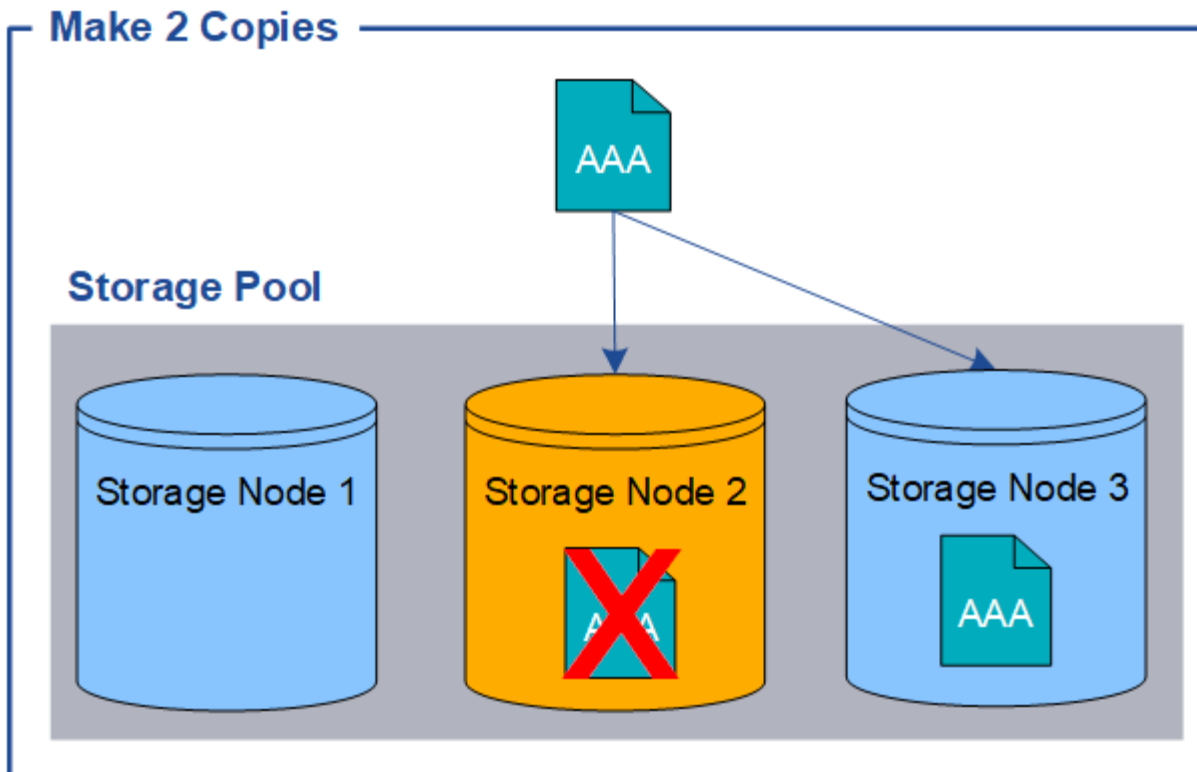


Quando uma regra ILM cria apenas uma cópia replicada de um objeto, o objeto fica inacessível quando o Storage Node está indisponível. Neste exemplo, você perderá temporariamente o acesso ao objeto AAA sempre que o Storage Node 2 estiver offline, como durante uma atualização ou outro procedimento de manutenção.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

Make 1 Copy



Para evitar a perda de dados de objetos, você deve sempre criar pelo menos duas cópias de todos os objetos que deseja proteger com replicação. Se existirem duas ou mais cópias, você ainda pode acessar o objeto se um Storage Node falhar ou ficar offline.



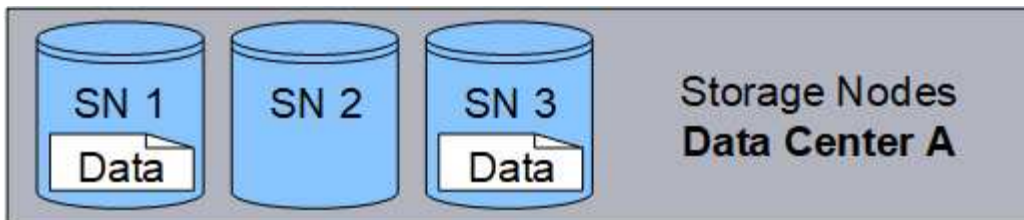
Saiba mais sobre codificação de apagamento no StorageGRID

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

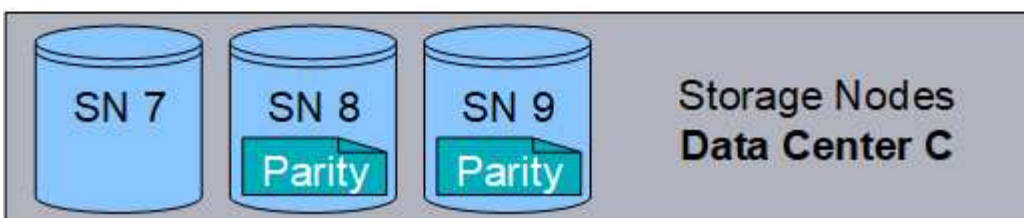
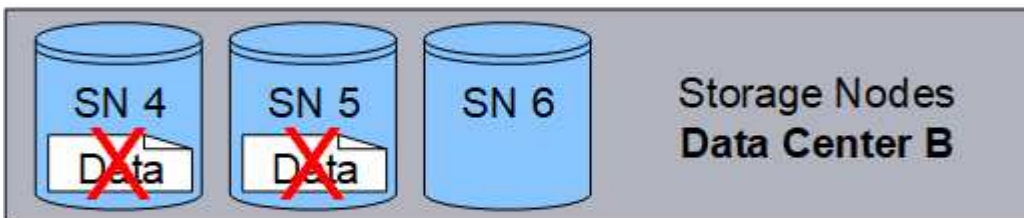
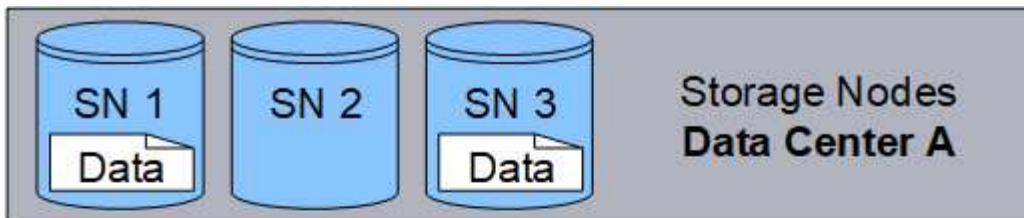
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um fragmento de dados ou de paridade for corrompido ou perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos fragmentos de dados e de paridade restantes.

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

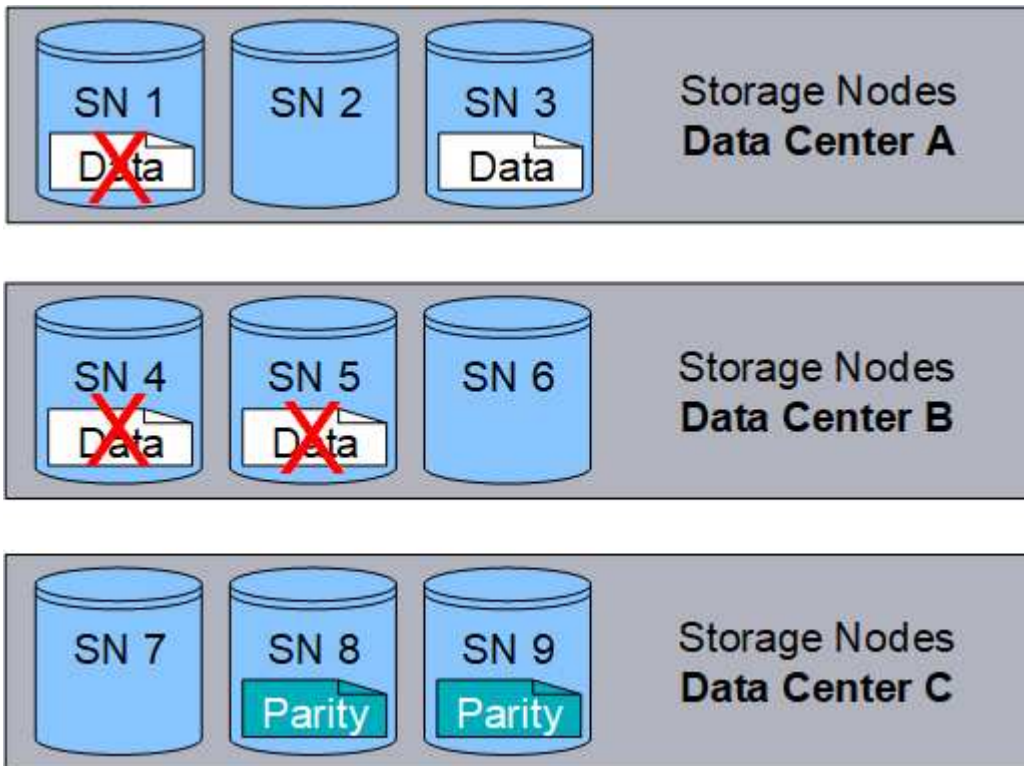
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM utiliza um esquema de codificação de apagamento 4+2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são calculados a partir dos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



O esquema de codificação de apagamento 4+2 pode ser configurado de diversas maneiras. Por exemplo, você pode configurar um pool de storage que contenha seis Storage Nodes. Para "[proteção contra perda de site](#)", você pode usar um pool de storage contendo três sites com três Storage Nodes em cada site. Um objeto pode ser recuperado desde que qualquer quatro dos seis fragmentos (dados ou paridade) permaneçam disponíveis. Até dois fragmentos podem ser perdidos sem perda dos dados do objeto. Se um site inteiro for perdido, o objeto ainda 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 storage"](#)
- ["O que são esquemas de codificação de apagamento"](#)
- ["Renomear um perfil de codificação de apagamento"](#)
- ["Desativar um perfil de codificação de apagamento"](#)

Saiba mais sobre esquemas de codificação de apagamento em StorageGRID

Os esquemas de codificação de apagamento 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 apagamento disponível. StorageGRID cria automaticamente esquemas de codificação de apagamento com base na quantidade de Storage Nodes e sites que compõem o pool de storage que você planeja usar.

Proteção de dados

O sistema StorageGRID utiliza o algoritmo de codificação de apagamento Reed-Solomon. O algoritmo divide um objeto em k fragmentos de dados e calcula m fragmentos de paridade.

Os $k + m = n$ fragmentos são distribuídos entre n Storage Nodes para fornecer proteção de dados da seguinte forma:

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

tolerância a falhas.

A melhor proteção de dados é fornecida pelo esquema de codificação de apagamento com a maior tolerância a falhas de nós ou volumes dentro de um pool de storage.

Sobrecarga de storage

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

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

Por exemplo, se você armazenar um objeto de 10 MB usando o esquema 4+2 (que tem 50% de sobrecarga de storage), o objeto consumirá 15 MB de storage em grade. Se você armazenar o mesmo objeto de 10 MB usando o esquema 6+2 (que tem 33% de sobrecarga de storage), 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 a adição de menos nós em um ["expansão quando for necessário mais storage"](#)

Diretrizes para pools de storage

Ao selecionar o pool de storage a ser usado para uma regra que criará uma cópia com codificação de apagamento, utilize as seguintes diretrizes para pools de storage:

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



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

- [Esquemas de codificação de apagamento para pools de storage contendo três ou mais sites](#)
- [Esquemas de codificação de apagamento para pools de storage de um único local](#)
- Não utilize um pool de storage que inclua o site All Sites.
- O pool de storage deve incluir pelo menos $k+m + 1$ Storage Nodes que possam armazenar dados de objetos.



Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados ("nó de armazenamento combinado"), apenas metadados de objetos ou apenas 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 acúmulo de ILM caso um nó de armazenamento necessário esteja temporariamente indisponível.

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

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

Para esquemas de codificação de apagamento que oferecem proteção contra perda de site, o número recomendado de nós de armazenamento no pool de storage 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 Storage Nodes em cada site	Número total recomendado de Storage Nodes	Proteção contra perda de site?	Sobrecarga de storage
4+2	3	3	9	Sim	50%
6+2	4	3	12	Sim	33%
8+2	5	3	15	Sim	25%
6+3	3	4	12	Sim	50%
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%



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

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

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

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



Se você 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 apagamento para pools de storage de um único local

Um pool de storage de um único site suporta todos os esquemas de codificação de apagamento definidos para três ou mais sites, desde que o site tenha Storage Nodes suficientes.

O número mínimo de Storage Nodes necessários é $k+m$, mas recomenda-se um pool de storage com $k+m + 1$ Storage Nodes. Por exemplo, o esquema de codificação de apagamento 2+1 requer um pool de storage com um mínimo de três Storage Nodes, mas recomenda-se quatro Storage Nodes.

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

Vantagens, desvantagens e requisitos para codificação de apagamento no StorageGRID

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

Vantagens da codificação de apagamento

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

- **Confiabilidade:** medida pelo número de falhas simultâneas que podem ser suportadas sem perda de dados.
 - Replicação: múltiplas cópias idênticas de um mesmo objeto são armazenadas em nós diferentes e em vários locais.
 - Codificação de apagamento: um objeto é codificado em fragmentos de dados e paridade e distribuído por vários nós e locais. Essa dispersão oferece proteção contra falhas tanto do local quanto do nó.
- **Disponibilidade:** A capacidade de recuperar objetos caso os Storage Nodes falhem ou se tornem inacessíveis. Em comparação com a replicação, codificação de apagamento oferece maior disponibilidade a custos de storage comparáveis.
- **Eficiência de storage:** Para disponibilidade e confiabilidade semelhantes, objetos com codificação de apagamento usam menos espaço de disco do que objetos replicados. Por exemplo, um objeto de 10 MB replicado em dois sites consome 20 MB de espaço de disco (duas cópias), enquanto um objeto com codificação de apagamento em três sites usando um esquema de codificação de apagamento 6+3 consome apenas 15 MB de espaço de disco.



O espaço em disco para objetos com codificação de apagamento é calculado como o tamanho do objeto mais a sobrecarga de storage. A porcentagem de sobrecarga de storage é o número de fragmentos de paridade dividido pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Em comparação com a replicação, a codificação de apagamento apresenta as seguintes desvantagens:

- É recomendável aumentar o número de Storage Nodes e sites, dependendo do esquema de codificação de apagamento. Por outro lado, se você replicar dados de objetos, precisará apenas de um Storage Node para cada cópia. Consulte ["Esquemas de codificação de apagamento para pools de storage contendo três ou mais sites"](#) e ["Esquemas de codificação de apagamento para pools de storage de um único local"](#).
- Aumento do custo e da complexidade das expansões de armazenamento. Para expandir uma implementação que usa replicação, você adiciona capacidade de storage em todos os locais onde as cópias de objetos são feitas. Para expandir uma implementação que usa codificação de apagamento, você deve considerar tanto o esquema de codificação de apagamento em uso quanto o nível de ocupação dos Storage Nodes existentes. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, precisará adicionar pelo menos $k+m$ Storage Nodes, mas se você expandir quando os nós existentes estiverem 70% cheios, poderá adicionar dois nós por site e ainda maximizar a capacidade de storage. Para obter mais informações, consulte ["Adicionar capacidade de storage para objetos com codificação de apagamento"](#).
- Há um aumento na latência de recuperação quando você utiliza codificação de apagamento em sites geograficamente distribuídos. Os fragmentos de um objeto que é codificado por apagamento e distribuído em sites remotos levam mais tempo para serem recuperados por conexões WAN do que um objeto que é replicado e está disponível localmente (no mesmo site ao qual o cliente se conecta).
- Ao utilizar codificação de apagamento em locais geograficamente distribuídos, 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.
- Ao usar codificação de apagamento entre sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência de rede entre os sites aumenta. Essa diminuição resulta da redução na taxa de transferência da rede TCP, o que afeta a velocidade com que o sistema StorageGRID consegue armazenar e recuperar fragmentos de objetos.
- Maior utilização de recursos computacionais.

Quando usar codificação de apagamento

Utilize codificação de apagamento para os seguintes requisitos:

- Objetos com tamanho superior a 1 MB.



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

- Armazenamento a longo prazo ou cold storage para conteúdo acessado com pouca frequência.
- Alta disponibilidade de dados e confiabilidade.
- Proteção contra falhas totais de site e nó.
- Eficiência de storage.
- Implantações em um único local que exigem proteção de dados eficiente com apenas uma única cópia com codificação de apagamento, em vez de várias cópias replicadas.
- Implantações em múltiplos locais onde a latência entre sites é inferior a 100 ms.

Como StorageGRID determina a retenção de objetos

StorageGRID oferece opções para que tanto os administradores do grid quanto os usuários individuais especifiquem por quanto tempo os objetos devem ser armazenados. Em geral, quaisquer instruções de retenção fornecidas por um usuário têm precedência sobre as instruções de retenção fornecidas pelo administrador do grid.

Como os usuários locatários controlam a retenção de objetos

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

- Se a configuração global de S3 Object Lock estiver habilitada para o grid, os usuários do tenant S3 podem criar buckets com S3 Object Lock ativado e, em seguida, selecionar um **período de retenção padrão** para cada bucket.
- Se a configuração global de S3 Object Lock estiver habilitada para o grid, os usuários do tenant S3 podem criar buckets com S3 Object Lock ativado e, em seguida, usar a API REST do S3 para especificar retain-until-date e as configurações de legal hold para cada versão de objeto adicionada a esse bucket.
 - Uma versão de objeto que esteja sob guarda legal não pode ser excluída por nenhum método.
 - Antes que a data de retenção de uma versão de objeto seja atingida, essa versão não pode ser excluída por nenhum método.
 - Os objetos em buckets com o S3 Object Lock ativado são retidos pelo ILM "para sempre". No entanto, após a data de retenção ser atingida, uma versão do objeto pode ser excluída por uma solicitação do cliente ou pelo término do ciclo de vida do bucket. Consulte ["Gerencie objetos com S3 Object Lock"](#).
- Os usuários locatários do S3 podem adicionar uma configuração de ciclo de vida aos seus buckets que especifica uma ação de Expiração. Se um ciclo de vida do bucket existir, o StorageGRID armazena um objeto até que a data ou o número de dias especificados na ação de Expiração sejam atingidos, a menos que o cliente exclua o objeto primeiro. Consulte ["Criar configuração de ciclo de vida do S3"](#).
- Um cliente S3 pode emitir uma solicitação de exclusão de objeto. StorageGRID sempre prioriza as solicitações de exclusão do cliente em relação ao ciclo de vida do bucket S3 ou ao ILM ao determinar se

deve excluir ou reter um objeto.

Como os administradores de grids controlam a retenção de objetos

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

- Defina um período máximo de retenção do S3 Object Lock para cada locatário. Em seguida, os usuários do locatário 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 (retain-until-date do objeto).
- Crie instruções de posicionamento ILM para controlar por quanto tempo os objetos são armazenados. Quando os objetos correspondem a uma regra ILM, StorageGRID armazena esses objetos até que o último período de tempo na regra ILM tenha expirado. Os objetos são retidos indefinidamente se "forever" for especificado para as 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 de apagamento) são armazenadas e onde as cópias estão localizadas (Storage Nodes ou Cloud Storage Pools).

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

Quando um ciclo de vida de bucket S3 é configurado, as ações de expiração do ciclo de vida substituem a política de ILM para objetos que correspondem ao filtro de ciclo de vida. Como resultado, um objeto pode ser retido no grid mesmo após o vencimento de quaisquer instruções de ILM para alocar o objeto.

Exemplos de retenção de objeto

Para melhor compreender as interações entre S3 Object Lock, as configurações de 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 do que o ILM

ILM

Armazene duas cópias por 1 ano (365 dias)

Ciclo de vida do bucket

Expirar objetos em 2 anos (730 dias)

Resultado

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



Se o ciclo de vida do bucket especificar que os objetos devem ser mantidos por mais tempo do que o especificado pelo ILM, StorageGRID continuará usando 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 sendo armazenadas no StorageGRID do dia 366 ao dia 730.

Exemplo 2: ciclo de vida do bucket S3 expira os 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

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

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

ILM

Armazene duas cópias em Storage Nodes "para sempre"

Ciclo de vida do bucket

Expirar objetos em 2 anos (730 dias)

Solicitação de exclusão do cliente

Emitido no dia 400

Resultado

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

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

Bloqueio de objeto S3

A data limite de retenção para uma versão do objeto é 31/03/2026. Não há guarda legal em vigor.

Regra ILM compatível

Armazene duas cópias em Storage Nodes "para sempre"

Solicitação de exclusão do cliente

Emitido em 31/03/2024

Resultado

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

Como StorageGRID exclui objetos

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

StorageGRID pode usar um dos dois métodos para excluir objetos:

- **Exclusão síncrona:** Quando 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 a remoção das cópias.
- **Os objetos são enfileirados para exclusão:** quando StorageGRID recebe uma solicitação de exclusão, o objeto é enfileirado para exclusão e o cliente é informado imediatamente de que a exclusão foi bem-sucedida. As cópias dos objetos são removidas posteriormente pelo processamento ILM em segundo

plano.

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

A tabela resume quando StorageGRID utiliza cada método.

Método de realização da exclusão	Quando usado
Os objetos são enfileirados para exclusão	Quando qualquer uma 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 S3 é alcançado. ◦ O último período de tempo especificado em uma regra ILM expira. • Um cliente S3 solicita a 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. Nota: Os objetos em um bucket com o S3 Object Lock ativado não podem ser excluídos se estiverem sob guarda legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida.
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 para processar.

Quando os clientes do S3 fazem solicitações de exclusão, StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, passa a realizar a exclusão síncrona. Garantir que a fila de exclusão em segundo plano tenha objetos para processar permite que o StorageGRID processe exclusões com mais eficiência, especialmente para clientes com baixa concorrência, além de ajudar a evitar o acúmulo de exclusões por parte dos clientes.

Tempo necessário para excluir objetos

A forma como o StorageGRID exclui objetos pode afetar como o sistema aparenta funcionar:

- Quando StorageGRID realiza a exclusão síncrona, pode levar até 30 segundos para que StorageGRID retorne 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 StorageGRID coloca objetos em fila para exclusão.
- Se você estiver monitorando atentamente o desempenho de exclusão durante uma exclusão em massa, pode notar que a taxa de exclusão parece diminuir após um certo número de objetos terem sido excluídos. Essa mudança ocorre quando StorageGRID passa de enfileirar objetos para exclusão para realizar a exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias dos objetos

estejam 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 os objetos em vez de excluí-los usando o ILM ou outros métodos. Em geral, o espaço é liberado mais rapidamente quando a exclusão é realizada pelos clientes, pois 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 se são 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 as cópias dos objetos são enfileiradas para remoção (tanto para exclusões feitas pelo cliente quanto por outros métodos).

Como os objetos versionados do S3 são excluídos

Quando o versionamento está habilitado para um bucket do S3, StorageGRID segue o comportamento do Amazon S3 ao responder a solicitações de exclusão, independentemente de essas solicitações virem de um cliente S3, do vencimento do ciclo de vida de um bucket S3 ou dos requisitos da política de ILM.

Quando os objetos são versionados, as solicitações de exclusão de objetos não excluem a versão atual do objeto e não liberam espaço livre. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão de zero bytes 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.

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

Se um cliente excluir uma versão de objeto com um ID de versão de um ["bucket de branch"](#) bucket de branch, StorageGRID oculta a existência da versão do objeto, mas não cria um marcador de exclusão no bucket de branch. Se um cliente excluir um objeto sem um ID de versão de um bucket de branch, StorageGRID cria um marcador de exclusão no bucket de branch de acordo com o comportamento padrão do S3.

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

- **Solicitação do cliente S3:** Especifique o ID da versão do objeto na solicitação DELETE Object do S3 (DELETE /object?versionId=ID). Lembre-se de que esta solicitação remove apenas as cópias do objeto para a versão especificada (as outras versões ainda ocupam espaço).
- **Bucket lifecycle:** Use a ação NoncurrentVersionExpiration na configuração do ciclo de vida do bucket. Quando o número de NoncurrentDays especificado for atingido, StorageGRID remove permanentemente todas as cópias de versões de objeto não atuais. Essas versões de objeto não podem ser recuperadas.

A `NewerNoncurrentVersions` ação na configuração do ciclo de vida do bucket especifica o número de versões não atuais retidas em um bucket S3 versionado. Se houver mais versões não atuais do que `NewerNoncurrentVersions` especificado, StorageGRID remove as versões mais antigas quando o valor de NoncurrentDays expirar. O `NewerNoncurrentVersions` limite substitui as regras de ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do

`NewerNoncurrentVersions` limite é retido se o ILM solicitar sua exclusão.

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

- **ILM:** ["Clonar uma política ativa"](#) e adicione duas regras ILM à nova política:
 - Primeira regra: Use "Tempo não atual" como Tempo 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 do objeto (em buckets do S3 com versionamento ativado)?"
 - Segunda regra: Use o **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** que corresponda aos marcadores de exclusão atuais. Os marcadores de exclusão são removidos somente quando um **Período de tempo** de **Dias** tiver decorrido e o marcador de exclusão atual tiver expirado (não existem versões não atuais).

- **Excluir objetos no bucket:** Use o gerenciador de locatários para ["Excluir todas as versões do objeto"](#) excluir objetos, incluindo marcadores de exclusão, de um bucket.

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

- Marcadores de exclusão criados no StorageGRID 11.7 ou anterior só podem ser removidos por solicitações do cliente S3; eles não são removidos pelo ILM, pelas regras de ciclo de vida do bucket ou pelas operações de exclusão de objetos no bucket.
- Marcadores de exclusão de um bucket criado no StorageGRID 11.8 ou posterior podem ser removidos pelo gerenciamento do ciclo de vida das informações (ILM), regras de ciclo de vida do bucket, operações de exclusão de objetos no bucket ou por uma exclusão explícita pelo cliente S3.

Informações relacionadas

- ["Utilize a API REST S3"](#)
- ["Exemplo 4: regras e políticas do ILM para objetos versionados do S3"](#)

Crie e atribua níveis de storage no StorageGRID

Os níveis de armazenamento identificam o tipo de armazenamento usado por um Nó de Armazenamento. Você pode criar níveis de armazenamento se desejar que as regras do ILM aloquem determinados objetos em Nós de Armazenamento específicos.

Antes de começar

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

Sobre esta tarefa

Ao instalar StorageGRID, a classificação de storage **Default** é atribuída automaticamente a cada Storage Node do seu sistema. Conforme necessário, você pode definir classificações de storage personalizadas e atribuí-las a diferentes Storage Nodes.

O uso de níveis de armazenamento personalizados permite criar pools de storage ILM que contenham apenas um tipo específico de Storage Node. Por exemplo, você pode querer que determinados objetos sejam armazenados nos seus Storage Nodes mais rápidos, como os appliances de storage all-flash StorageGRID.



Nós de storage somente de metadados não podem ter uma classificação de storage atribuída. Para obter mais informações, consulte ["Tipos de nós de armazenamento"](#).

Se a classificação de armazenamento não for uma preocupação (por exemplo, se todos os Storage Nodes forem idênticos), você pode ignorar este procedimento e usar a opção **inclui todas as classificações de armazenamento** para a classificação de armazenamento quando você ["criar pools de storage"](#). Usar essa opção garante que o pool de storage incluirá todos os Storage Nodes no site, independentemente de sua classificação de armazenamento.



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

Passos

1. Selecione **ILM > Storage grades**.
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.



Storage Grades

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

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

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

Apply Changes

c. Selecione **Aplicar alterações**.

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



Você não pode excluir níveis de armazenamento.

3. Atribua novas categorias de armazenamento aos nós de armazenamento:

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

b. Selecione a classe de armazenamento apropriada na lista.



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

Apply Changes



Atribua um storage grade a um determinado Storage Node apenas uma vez. Um Storage Node recuperado de uma falha mantém o storage grade atribuído anteriormente. Não altere essa atribuição após a ativação da política de ILM. Se a atribuição for alterada, os dados serão armazenados com base no novo storage grade.

a. Selecione **Aplicar alterações**.

Utilize pools de storage

Saiba mais sobre pool de storage no StorageGRID

Um pool de storage é um agrupamento lógico de Storage Nodes.

Ao instalar StorageGRID, um pool de storage por site é criado automaticamente. Você pode configurar pools de storage adicionais conforme necessário para atender às suas necessidades de armazenamento.



Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados ("nó de armazenamento combinado"), apenas metadados de objetos ou apenas dados de objetos. Nós de armazenamento somente com metadados não podem ser usados em pool de storage. Para mais informações, consulte ["Tipos de nós de armazenamento"](#).

Os pools de storage possuem dois atributos:

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

Os pools de armazenamento são usados nas regras do ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar as regras do ILM para replicação, você seleciona um ou mais pools de armazenamento.

Diretrizes de configuração do pool de storage no StorageGRID

Configure e utilize pools de storage para proteger contra perda de dados distribuindo os dados por vários sites. Cópias replicadas e cópias com codificação de apagamento exigem diferentes configurações de pool de storage.

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

Diretrizes para todos os pools de storage

- Mantenha as configurações do pool de storage o mais simples possível. Não crie mais pools de storage do que o necessário.
- Crie pools de storage com o máximo de nós possível. Cada pool de storage deve conter dois ou mais nós. Um pool de storage com nós insuficientes pode causar atrasos no ILM se um nó ficar indisponível.
- Evite criar ou usar pools de storage que se sobreponham (contenham um ou mais dos mesmos nós). Se pools de storage se sobrepuserem, mais de uma cópia dos dados do objeto pode ser salva no mesmo nó.
- Em geral, não utilize o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores) nem 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 que você deseja.

Diretrizes para pools de storage usados para cópias replicadas

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

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

Utilizar um pool de storage para cada site garante que as cópias replicadas dos objetos 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 storage que contenha apenas o novo site. Em seguida, ["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 storage, o sistema distribui as cópias para equilibrar o uso do disco entre os pools.
- Se os pools de armazenamento se sobrepuserem (contiverem os mesmos Storage Nodes), 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 Storage Nodes.

Diretrizes para pools de storage usados para cópias com codificação de apagamento

- Para proteção contra perda de sites usando ["codificação de apagamento"](#), crie pools de storage que consistam em pelo menos três sites. Se um pool de storage incluir apenas dois sites, você não pode usar esse pool de storage para codificação de apagamento. Nenhum esquema de codificação de apagamento está disponível para um pool de storage que tenha dois sites.
- O número de nós de armazenamento e sites contidos no pool de storage determina quais ["esquemas de codificação de apagamento"](#) estão disponíveis.
- Se possível, um pool de storage deve incluir mais do que o número mínimo de Storage Nodes exigido pelo esquema de codificação de apagamento que você selecionar. Por exemplo, se você usar um esquema de codificação de apagamento 6+3, será necessário ter pelo menos nove Storage Nodes. No entanto,

recomenda-se ter pelo menos um Storage Node adicional por site.

- Distribua os nós de armazenamento entre os locais da forma mais uniforme possível. Por exemplo, para suportar um esquema de codificação de apagamento 6+3, configure um pool de storage que inclua pelo menos três nós de armazenamento em três locais.
- Se você tiver requisitos de taxa de transferência elevados, não é recomendável usar um pool de storage que inclua vários sites se a latência de rede entre os sites for superior a 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 redução na taxa de transferência da rede TCP.

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



Se sua grade incluir apenas um site, você ficará impedido de usar o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores) ou o site All Sites em um perfil de codificação de apagamento. Esse comportamento impede que o perfil se torne inválido caso um segundo site seja adicionado.

Proteção contra perda de sites com pools de storage no StorageGRID

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

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

- Para usar a replicação para proteção contra perda de site, use os pools de storage específicos do site que são criados automaticamente durante a instalação do StorageGRID. Em seguida, crie regras ILM com ["instruções de colocação"](#) que especifiquem vários pools de storage, para que uma cópia de cada objeto seja colocada em cada site.
- Para usar codificação de apagamento para proteção contra perda de sites, ["Criar pools de storage que consistem em vários sites"](#). Em seguida, crie regras ILM que usem um pool de storage composto por vários sites e qualquer esquema de codificação de apagamento disponível.



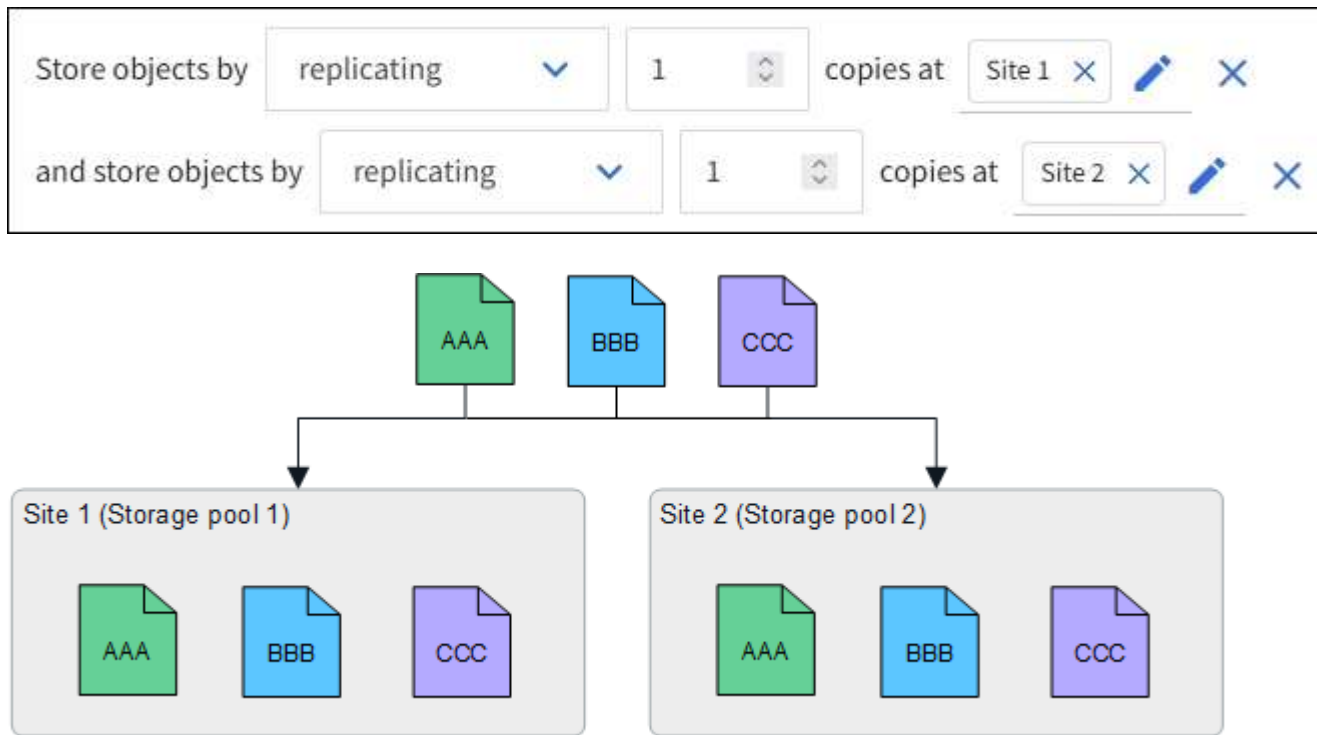
Ao configurar sua implantação do StorageGRID para proteção contra perda de site, você também deve levar em consideração os efeitos de ["opções de ingestão"](#) e ["consistência"](#).

Exemplo de replicação

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

- O pool de storage 1 contém o Site 1
- O pool de storage 2 contém Site 2
- A regra ILM contém duas colocações:
 - Armazene objetos replicando 1 cópia no Site 1
 - Armazene objetos replicando 1 cópia no Site 2

Posicionamento das regras de ILM:



Caso um dos locais seja perdido, cópias dos objetos estão disponíveis no outro local.

Exemplo de codificação de apagamento

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

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

Posicionamento das regras de ILM:



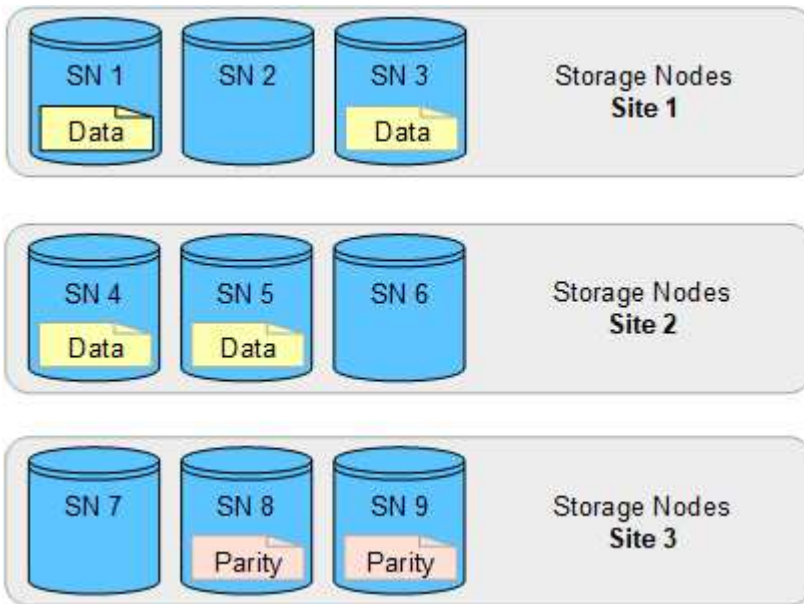
Neste exemplo:

- A regra ILM utiliza um esquema de codificação de apagamento 4+2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são calculados a partir dos dados do objeto.
- Cada um dos seis fragmentos é armazenado em um nó diferente em três sites de data center para fornecer proteção de dados em caso de falhas de nó ou perda de site.

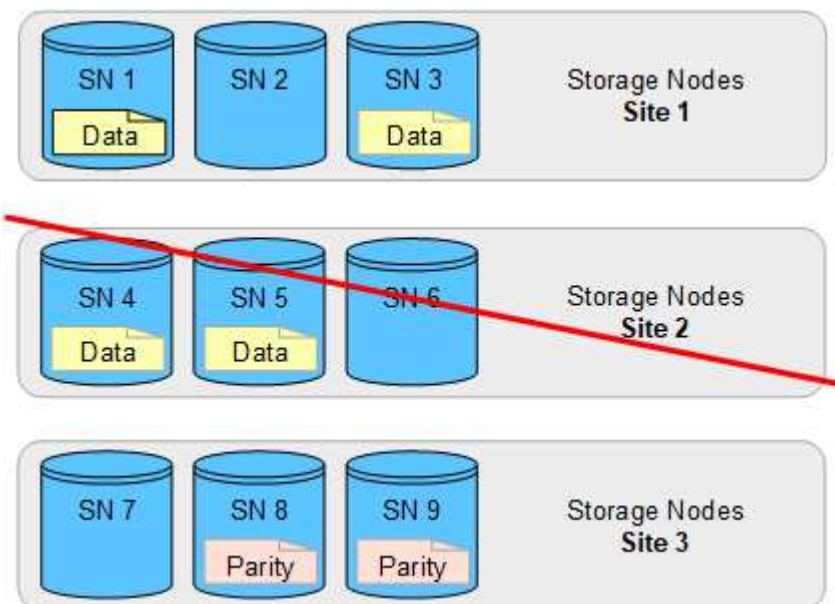


A codificação de apagamento é permitida em pools de storage que contenham qualquer número de sites, *exceto* dois sites.

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



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



Crie um pool de storage no StorageGRID

Você cria pools de storage para determinar onde o StorageGRID armazena os dados dos objetos e o tipo de storage utilizado. Cada pool de storage inclui um ou mais sites e um ou mais storage grades.



Ao instalar StorageGRID 12.0 em uma nova grid, os pools de storage são criados automaticamente para cada site. No entanto, se você instalou inicialmente StorageGRID 11.6 ou uma versão anterior, os pools de storage não são criados automaticamente para cada site.

Se você deseja criar Cloud Storage Pools para armazenar dados de objetos fora do seu sistema StorageGRID, consulte o ["Informações sobre como usar os Cloud Storage Pools"](#).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você já analisou as diretrizes para a criação de pools de storage.

Sobre esta tarefa

Os pools de storage determinam onde os dados dos objetos são armazenados. O número de pools de storage que você precisa depende da quantidade de sites em seu grid e dos tipos de cópias que você deseja: replicadas ou com codificação de apagamento.

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



Não inclua o site "All Sites" em um pool de storage que será usado em um perfil de codificação de apagamento. Em vez disso, adicione uma entrada separada ao pool de storage para cada site que armazenará dados codificados por apagamento. Veja [esta etapa](#) para um exemplo.

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

Passos

1. Selecione **ILM > pool de storage**.

A aba "Pools de storage" lista todos os pools de storage definidos.



Para novas instalações do StorageGRID 11.6 ou anterior, o pool de storage All Storage Nodes é atualizado automaticamente sempre que você adiciona novos sites de data center. Não utilize este pool em regras ILM.

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

Ao selecionar um site, o número de nós de Storage Nodes na tabela é atualizado automaticamente.

Em geral, não utilize o site "All Sites" em nenhum pool de storage. As regras do ILM que utilizam um pool de storage All Sites alocam objetos em qualquer site disponível, reduzindo seu controle sobre a alocação de objetos. Além disso, um pool de storage All Sites utiliza os Storage Nodes em um novo site imediatamente, o que pode não ser o comportamento que você espera.

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

A categoria de armazenamento, *inclui todas as categorias de armazenamento*, engloba todos os Storage Nodes no site selecionado. Se você criou categorias de armazenamento adicionais para os Storage

Nodes em sua grid, elas serão listadas no menu suspenso.

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



Você será avisado se adicionar mais de uma entrada com diferentes grades de storage para um site.

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

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

O novo pool de storage é adicionado à lista.

Veja os detalhes do pool de storage no StorageGRID

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

Antes de começar

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

Passos

1. Selecione **ILM > pool de storage**.

A tabela de pools de storage inclui as seguintes informações para cada pool de storage que inclui Storage Nodes:

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

2. Para visualizar os detalhes de um pool de storage específico, selecione o nome dele.

A página de detalhes do pool de storage é exibida.

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

A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do site
- Grau de storage

- Utilização do armazenamento: a porcentagem do espaço total utilizável para dados de objetos que foi utilizada pelo Nó de Armazenamento.



O mesmo valor de uso de storage (%) também é exibido no gráfico "Storage Utilizado - Dados do Objeto" para cada Storage Node (selecione **Nodes > Storage Node > Storage**).

4. Consulte a guia **Uso do ILM** para determinar se o pool de storage está sendo usado em alguma regra do ILM ou perfil de codificação de apagamento.
5. Opcionalmente, acesse a **página de regras do ILM** para saber mais e gerenciar quaisquer regras que utilizam o pool de storage.

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

Editar um pool de storage no StorageGRID

Você pode editar um pool de storage para alterar seu nome ou atualizar sites e storage grades.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem "[permissões de acesso específicas](#)".
- Você revisou o "[diretrizes para a criação de pools de storage](#)".
- Se você planeja editar um pool de storage usado por uma regra na política ILM ativa, você já considerou 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 storage usado na política ILM ativa, esteja ciente de que os Storage Nodes 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 ILM após salvar o pool de storage editado.

Passos

1. Selecione **ILM > pool de storage**.
2. Selecione a caixa de seleção correspondente ao pool de storage que você deseja editar.

Você não pode editar o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores).

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

Você está impedido de alterar o site ou o nível de armazenamento se o pool de storage for usado em um perfil de codificação de apagamento e a alteração invalidar o esquema de codificação de apagamento. Por exemplo, se um pool de storage usado em um perfil de codificação de apagamento incluir atualmente um nível de armazenamento com apenas um site, você está impedido de usar um nível de armazenamento com dois sites porque a alteração invalidaria o esquema de codificação de apagamento.



Adicionar ou remover sites de um pool de storage existente não moverá nenhum dado já codificado por apagamento. Se você quiser mover os dados existentes do site, será necessário criar um novo pool de storage e um novo perfil de 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 storage usado na política ILM ativa, ative uma nova política ILM para forçar o StorageGRID a usar o novo site ou nível de armazenamento. Por exemplo, clone sua política ILM existente e depois ative o clone. Consulte ["Trabalhe com regras e políticas do ILM"](#).

Remover um pool de storage no StorageGRID

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

Antes de começar

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

Passos

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

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

3. Se o pool de storage que você deseja remover não estiver sendo usado, selecione a caixa de seleção.
4. Selecione **Remove**.
5. Selecione **OK**.

Use Cloud Storage Pools

Saiba mais sobre Cloud Storage Pools no StorageGRID

Um pool de storage 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 storage de nuvem de menor custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a camada de acesso Archive no Microsoft Azure Blob storage. Ou, você pode querer manter um backup em nuvem dos objetos do StorageGRID para aprimorar a recuperação de desastres.

Do ponto de vista do ILM, um pool de storage de nuvem é semelhante a um pool de storage. Para armazenar objetos em qualquer um dos locais, você seleciona o pool ao criar as instruções de posicionamento para uma regra do ILM. No entanto, enquanto os pools de storage consistem em Storage Nodes dentro do sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo (S3) ou contêiner (Azure Blob storage).

A tabela compara os pools de storage com os Cloud Storage Pools e mostra as semelhanças e diferenças de alto nível.

	Pool de storage	Pool de storage em nuvem
Como é criado?	Utilizando a opção ILM > Pools de storage no Grid Manager.	Utilizando a opção ILM > Storage pools > Cloud Storage Pools no Grid Manager. Você precisa configurar o bucket ou contêiner externo antes de criar o Cloud Storage Pool.
Quanto pools você pode criar?	Ilimitado.	Até 10.
Onde os objetos são armazenados?	Em um ou mais nós de armazenamento dentro do StorageGRID.	Em um bucket do Amazon S3, um contêiner do Azure Blob storage ou um serviço do Google Cloud que é externo ao sistema StorageGRID. Se o pool de storage de nuvem for um bucket do Amazon S3: • Opcionalmente, você pode configurar um ciclo de vida do bucket para transferir objetos para storage de longo prazo e baixo custo, como Amazon S3 Glacier ou S3 Glacier Deep Archive. O sistema de storage externo deve ser compatível com a classe de storage Glacier e com a API S3 RestoreObject. • Você pode criar Cloud Storage Pools para uso com AWS Commercial Cloud Services (C2S), que são compatíveis com AWS Secret Region. Se o pool de storage de nuvem for um contêiner de Azure Blob storage, StorageGRID faz a transição do objeto para a camada Archive. Observação: Em geral, não configure o gerenciamento de ciclo de vida do Azure Blob storage para o contêiner usado para um Cloud Storage Pool. 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 ILM nas políticas ILM ativas.	Uma regra ILM nas políticas ILM ativas.
Qual método de proteção de dados é usado?	Replicação ou codificação de apagamento.	Replicação.

	Pool de storage	Pool de storage em nuvem
Quantas cópias de cada objeto são permitidas?	Múltiplos.	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 storage de nuvem ao mesmo tempo.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Storage de baixo custo. Observação: os dados do FabricPool não podem ser organizados em camadas nos Cloud Storage Pools.

Ciclo de vida de um objeto de pool de storage em nuvem no StorageGRID

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 storage em nuvem

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



"Glacier" refere-se tanto à classe de armazenamento Glacier quanto à classe de armazenamento Glacier Deep Archive, com uma exceção: a classe de armazenamento Glacier Deep Archive não suporta o nível de restauração Expedited. Apenas a recuperação Bulk ou Standard é suportada.



A plataforma Google Cloud (GCP) suporta a recuperação de objetos do storage de longo prazo sem a necessidade de uma operação POST Restore.

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 storage em nuvem S3

- Quando o objeto é correspondido por uma regra ILM que usa um Cloud Storage Pool S3 como local de armazenamento, 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 migrado para o armazenamento Glacier.

3. Objeto transferido para o Glacier (estado não recuperável)

- Opcionalmente, o objeto pode ser transferido para o storage Glacier. Por exemplo, o bucket S3 externo pode usar a configuração de ciclo de vida para transferir um objeto para o storage Glacier imediatamente ou após um determinado número de dias.



Se você deseja realizar a transição de objetos, precisa criar uma configuração de ciclo de vida para o bucket S3 externo e usar uma solução de storage que implemente a classe de armazenamento Glacier e seja compatível com a API RestoreObject do S3.

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

4. Objeto restaurado do storage Glacier

Se um objeto tiver sido migrado para o storage Glacier, o aplicativo cliente pode emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o pool de storage em nuvem do S3. A solicitação especifica por quantos dias a cópia deve estar disponível no pool de storage em nuvem e o nível de acesso a dados a ser usado para a operação de restauração (Expedited, Standard ou Bulk). Quando a data de expiração da cópia recuperável for atingida, a cópia retorna automaticamente a um estado não recuperável.



Se uma ou mais cópias do objeto também existirem em Storage Nodes dentro do StorageGRID, não é necessário 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 for restaurado, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Azure: ciclo de vida de um objeto de pool de storage em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um pool de storage do Azure Cloud Storage.

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 storage em nuvem do Azure

Quando o objeto é correspondido por uma regra de ILM que usa um pool de storage em nuvem do Azure como local de colocação, StorageGRID move o objeto para o container de Azure Blob storage externo especificado pelo Cloud Storage Pool.

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

Imediatamente após mover o objeto para o pool de storage em nuvem do Azure, StorageGRID automaticamente transfere o objeto para a camada Archive do Azure Blob storage.

4. Objeto restaurado do nível Archive

Se um objeto tiver sido movido para a camada de Archive, o aplicativo cliente pode emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável no pool de storage em nuvem do Azure.

Quando StorageGRID recebe o RestoreObject, ele transiciona temporariamente o objeto para a camada Cool do Azure Blob storage. Assim que a data de expiração na solicitação RestoreObject é atingida, StorageGRID transiciona o objeto de volta para a camada Archive.



Se uma ou mais cópias do objeto também existirem em Storage Nodes dentro do StorageGRID, não é necessário restaurar o objeto da camada de acesso Archive 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 para o pool de storage em nuvem do Azure, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Informações relacionadas

["Utilize a API REST S3"](#)

Casos de uso do Cloud Storage Pool no StorageGRID

Usando os Cloud Storage Pools, você pode fazer backup ou armazenar dados em camadas em um local externo. Além disso, você pode fazer backup ou armazenar dados em camadas 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 podem ser usados para atender às solicitações do cliente. No entanto, talvez seja necessário emitir uma solicitação S3 RestoreObject para acessar a cópia de backup do objeto no Cloud Storage Pool.

Os dados de objeto em um Cloud Storage Pool também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha de volume de storage ou de Storage Node. Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID restaura temporariamente o objeto e cria uma nova cópia no Storage Node recuperado.

Para implementar uma solução de backup:

1. Crie um único Cloud Storage Pool.
2. Configure uma regra ILM que armazene simultaneamente cópias de objetos em Storage Nodes (como cópias replicadas ou com código de apagamento) e uma única cópia do objeto no Cloud Storage Pool.
3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Transferir dados de camada do StorageGRID para um 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 reter, mas espera acessá-los raramente, se é que vai acessá-los. Você pode usar um Cloud Storage Pool para transferir os objetos para um armazenamento de menor custo e liberar espaço no StorageGRID.

Para implementar uma solução de tiering:

1. Crie um único Cloud Storage Pool.
2. Configure uma regra ILM que mova objetos raramente usados dos Storage Nodes para o Cloud Storage Pool.

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

Manter vários endpoints na nuvem

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



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

Para implementar vários endpoints na nuvem:

1. Crie até 10 Cloud Storage Pools.
2. Configure as regras do ILM para armazenar os dados de objeto apropriados no momento apropriado em cada Cloud Storage Pool. Por exemplo, armazene objetos do bucket A em Cloud Storage Pool A e objetos do bucket B em Cloud Storage Pool B. Ou, armazene objetos em Cloud Storage Pool A por um determinado período e depois mova-os para Cloud Storage Pool B.
3. Adicione as regras à sua política ILM. Em seguida, simule e ative a política.

Requisitos e limites do Cloud Storage Pool no StorageGRID

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

Considerações gerais

- Em geral, o armazenamento em nuvem para arquivamento, como Amazon S3 Glacier ou Azure Blob storage, é uma opção econômica para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento em nuvem para arquivamento são relativamente altos. Para obter o menor custo total, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um Cloud Storage Pool é recomendado apenas para conteúdo que você espera acessar com pouca frequência.
- O uso de Cloud Storage Pools com FabricPool não é compatível 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 Cloud Storage Pools.
- As seguintes combinações de plataforma, autenticação e protocolo com o S3 Object lock não são compatíveis com Cloud Storage Pools:
 - **Plataformas:** Google Cloud Platform e Azure
 - **Tipos de autenticação:** acesso anônimo
 - **Protocolo:** HTTP

Considerações sobre as portas utilizadas para os Cloud Storage Pools

Para garantir que as regras do ILM possam mover objetos de e para o Cloud Storage Pool especificado, você deve configurar a(s) rede(s) que contém(êm) os Storage Nodes do seu sistema. Você deve garantir que as

seguintes portas possam se comunicar com o Cloud Storage Pool.

Por padrão, os Cloud Storage Pools 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 Cloud Storage Pool.

Se você utiliza um servidor proxy não transparente, também precisa "[configurar um servidor proxy de storage](#)" permitir que mensagens sejam enviadas para endpoints externos, como um endpoint na internet.

Considerações sobre custos

O acesso ao storage 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 espera mover entre StorageGRID e a nuvem usando o Cloud Storage Pool.

Quando StorageGRID se conecta ao endpoint externo do Cloud Storage Pool, ele emite várias solicitações para monitorar a conectividade e garantir que pode executar as operações necessárias. Embora alguns custos adicionais estejam associados a essas solicitações, o custo de monitorar um Cloud Storage Pool deve representar apenas uma pequena fração do custo total de armazenar objetos no S3 ou no Azure.

Custos mais significativos podem ser incorridos se você precisar mover objetos de um endpoint externo do Cloud Storage Pool de volta para StorageGRID. Objetos podem ser movidos de volta para StorageGRID em qualquer um destes casos:

- A única cópia do objeto está em um Cloud Storage Pool e você decide armazenar o objeto no StorageGRID em vez disso. Nesse caso, você reconfigura suas regras e políticas do ILM. Quando a avaliação do ILM ocorre, o StorageGRID faz várias solicitações para recuperar o objeto do Cloud Storage Pool. O StorageGRID então cria localmente o número especificado de cópias replicadas ou com código de eliminação. Depois que o objeto é movido de volta para o StorageGRID, a cópia no Cloud Storage Pool é excluída.
- Os objetos são perdidos devido a falha no Storage Node. Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID restaura temporariamente o objeto e cria uma nova cópia no Storage Node recuperado.



Quando objetos são movidos de volta para StorageGRID a partir de um Cloud Storage Pool, StorageGRID envia várias solicitações ao endpoint 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 tempo necessário e dos custos associados.

S3: permissões necessárias para o bucket do Cloud Storage Pool

As políticas do bucket S3 externo usado para um Cloud Storage Pool devem conceder ao StorageGRID permissão para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento Glacier quando necessário e mais. Idealmente, o StorageGRID deve ter acesso de controle total ao bucket (`s3:*`; no entanto, se isso não for possível, a política do 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 StorageGRID e o bucket S3 externo especificado no Cloud Storage Pool é controlada pelas regras de ILM e pelas políticas de ILM ativas no StorageGRID. Em contraste, a transição de objetos do bucket S3 externo especificado no Cloud Storage Pool para Amazon S3 Glacier ou S3 Glacier Deep Archive (ou para uma solução de storage que implemente a classe de armazenamento Glacier) é controlada pela configuração de ciclo de vida desse bucket.

Se você deseja migrar objetos do Cloud Storage Pool, é necessário criar a configuração de ciclo de vida apropriada no bucket S3 externo e usar uma solução de storage que implemente a classe de armazenamento Glacier e seja compatível com a API RestoreObject do S3.

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

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

Essa regra faria a transição de todos os objetos do bucket para o Amazon S3 Glacier no dia em que 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. As ações de Expiração fazem com que o sistema de storage externo exclua os objetos expirados. Se você tentar acessar um objeto expirado posteriormente no StorageGRID, o objeto excluído não será encontrado.

Se você deseja migrar 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 nível `Expedited` 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 Hot ou Cool. Ao criar uma conta de armazenamento para uso com um Cloud Storage Pool, você deve usar o nível Hot como padrão. Embora o StorageGRID defina imediatamente o nível como Archive ao mover objetos para o Cloud Storage Pool, usar a configuração padrão Hot garante que você não será cobrado por exclusão antecipada de objetos removidos do nível Cool antes do período mínimo de 30 dias.

Azure: gerenciamento de ciclo de vida não suportado

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

Informações relacionadas

["Criar um Cloud Storage Pool"](#)

Pools de armazenamento em nuvem e CloudMirror replication no StorageGRID

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 storage em nuvem	CloudMirror serviço de replicação
Qual é o objetivo principal?	Funciona como um destino de arquivamento. 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 localmente, 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 storage, usando o Grid Manager ou a Grid Management API. Pode ser selecionado como local de colocação em uma regra ILM. Enquanto um pool de storage consiste em um grupo de Storage Nodes, um Cloud Storage Pool é definido usando um endpoint remoto S3 ou Azure (endereço IP, credenciais e assim por diante).	Um usuário locatário " configura a replicação CloudMirror " define um endpoint CloudMirror (endereço IP, credenciais e assim por diante) usando o Gerenciador de Locatários ou a API S3. Depois que o endpoint CloudMirror é configurado, qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint CloudMirror.
Quem é responsável por configurá-lo?	Normalmente, um administrador de grid	Normalmente, um usuário tenant

	Pool de storage em nuvem	CloudMirror serviço de replicação
Qual é o destino?	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Camada de Arquivo de Blob do Azure - Google Cloud Platform (GCP)	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Google Cloud Platform (GCP)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras ILM nas políticas ILM ativas. As regras ILM definem quais objetos 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 CloudMirror. Objetos que já existiam no bucket de origem antes de o bucket ser configurado com o endpoint 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 Cloud Storage Pool. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivamento, 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 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.
É possível ler diretamente do destino?	Não. Os objetos movidos para um Cloud Storage Pool são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação a partir do Cloud Storage Pool).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da origem?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído deixa de existir no bucket do StorageGRID, mas continua existindo no bucket de destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.
Como você acessa objetos após um desastre (sistema StorageGRID inoperante)?	Os nós do StorageGRID com falha precisam ser recuperados. Durante esse processo, cópias de objetos replicados podem ser restauradas usando as cópias no Cloud Storage Pool.	As cópias dos objetos no destino CloudMirror são independentes do StorageGRID, então podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Criar um Cloud Storage Pool no StorageGRID

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

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

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 Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).
- Você revisou o ["Considerações sobre Cloud Storage Pools"](#).
- O bucket ou contêiner externo referenciado pelo Cloud Storage Pool já existe e você tem o [informações do endpoint de serviço](#).
- Para acessar o bucket ou container, você tem a [Informações da conta para o tipo de autenticação](#) que vai escolher.

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.
2. Selecione **Criar** e, em seguida, insira as seguintes informações:

Campo	Descrição
Nome do pool de storage em nuvem	Um nome que descreva brevemente o pool de storage em nuvem e sua finalidade. Use um nome que seja fácil de identificar ao configurar as regras de ILM.
Tipo de provedor	Qual provedor de nuvem você usará para este pool de storage 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. • Azure Blob Storage
Bucket ou container	O nome do bucket S3 externo ou do contêiner do Azure. Você não pode alterar esse valor depois que o pool de Cloud Storage é salvo.

3. Com base na sua seleção de tipo de provedor, insira as informações do endpoint de serviço.

Amazon S3/GCP

- a. Para o protocolo, selecione HTTPS ou HTTP.



Não utilize conexões HTTP para dados confidenciais.

- b. Digite o nome do host. Exemplo:

`s3-aws-region.amazonaws.com`

- c. Selecione o estilo da URL:

Opção	Descrição
Detecção automática	Tenta detectar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, StorageGRID usará uma URL no formato de caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Estilo virtual-hosted	Use uma URL no estilo de hospedagem virtual para acessar o bucket. URLs no estilo de hospedagem virtual incluem o nome do bucket como parte do nome de domínio. Exemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de caminho	Use uma URL no formato de caminho para acessar o bucket. URLs no formato de caminho incluem o nome do bucket no final. Exemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: A opção de URL no formato 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.

Azure Blob Storage

- a. Usando um dos seguintes formatos, insira o URI do endpoint 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 é usada para HTTPS e a porta 80 é usada para HTTP.

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

Chave de acesso

Para Amazon S3/GCP ou outro provedor compatível com S3

- a. **ID da chave de acesso:** Insira o ID da chave de acesso da conta proprietária do bucket externo.
- b. **Chave de acesso secreta:** Digite a chave de acesso secreta.

IAM Roles Anywhere

Para o serviço AWS IAM Roles Anywhere

StorageGRID utiliza 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 pool de storage em nuvem. Por exemplo, `us-east-1`.
- b. **URN da âncora de confiança:** Insira o URN da âncora de confiança que valida as 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 IAM que pode ser assumida 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 no máximo 12 horas.
- f. **Certificado de CA do servidor** (opcional): Um ou mais certificados de CA confiáveis, em formato PEM, para verificar o servidor IAM Roles Anywhere. Se omitido, o servidor não será verificado.
- g. **Certificado de entidade final:** A chave pública, em formato PEM, do certificado X509 assinado pela trust anchor. O AWS IAM Roles Anywhere usa essa chave para emitir um token STS.
- h. **Chave privada da entidade final:** a chave privada do certificado da entidade final.

CAP (portal de acesso C2S)

Para o serviço S3 de Commercial Cloud Services (C2S)

- a. **URL de credenciais temporárias:** Insira a URL completa que 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 StorageGRID usará para verificar o servidor CAP. O certificado deve estar codificado em PEM e ter sido emitido por uma Autoridade de Certificação (CA) governamental apropriada.
- c. **Certificado do cliente:** selecione **Procurar** e carregue o certificado que StorageGRID usará para se identificar no servidor CAP. O certificado do cliente deve estar codificado em PEM, ser emitido por uma Autoridade Certificadora (CA) governamental apropriada e ter permissão de acesso 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 descriptografar a chave privada do cliente. 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 compatível.

Azure Blob Storage

Somente para Azure Blob Storage, apenas com Shared Key

- Nome da conta:** Insira o nome da conta de armazenamento que é proprietária do contêiner externo
- Chave da conta:** Insira a chave secreta da conta de storage

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

6. Selecione **Salvar**.

Ao salvar um Cloud Storage Pool, StorageGRID faz o seguinte:

- Valida se o bucket ou contêiner e o endpoint do 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 Cloud Storage Pool. Nunca remova este arquivo, que tem o nome `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 que você especificou ainda não existir.

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

Veja os detalhes do Cloud Storage Pool no StorageGRID

Você pode visualizar os detalhes de um Cloud Storage Pool para determinar onde ele é usado e para ver quais nós e storage grades estão incluídos.

Antes de começar

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

Passos

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

A tabela de Cloud Storage Pools inclui as seguintes informações para cada Cloud Storage Pool que inclui Storage Nodes:

- **Nome:** O nome de exibição exclusivo do pool.
- **URI:** O Identificador Uniforme de Recursos do pool de storage de nuvem.
- **Tipo de provedor:** Qual provedor de nuvem é usado para este Cloud Storage Pool.
- **Contêiner:** O nome do bucket usado para o pool de storage de nuvem.
- **Uso do ILM:** Como o pool está sendo usado atualmente. Um Cloud Storage Pool pode estar ocioso ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de apagamento ou ambos.
- **Último erro:** O último erro detectado durante uma verificação de integridade deste pool de storage de nuvem.

2. Para visualizar os detalhes de um Cloud Storage Pool específico, selecione o nome dele.

A página de detalhes do pool é exibida.

3. Consulte a guia **Autenticação** para saber mais sobre o tipo de autenticação para este pool de storage em nuvem e para editar os detalhes de autenticação.
4. Consulte a aba **Verificação do servidor** para obter detalhes sobre a verificação, editar a verificação, baixar um novo certificado ou copiar o PEM do certificado.
5. Consulte a guia **Uso do ILM** para determinar se o Cloud Storage Pool está sendo usado em alguma regra de ILM ou perfil de codificação de apagamento.
6. Opcionalmente, acesse a **página de regras do ILM** para ["saiba mais e gerencie quaisquer regras"](#) que usam o pool de storage de nuvem.

Editar um Cloud Storage Pool no StorageGRID

Você pode editar um Cloud Storage Pool para alterar seu nome, endpoint de serviço ou outros detalhes; no entanto, não é possível alterar o bucket do S3 ou o container do Azure para um Cloud Storage Pool.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você revisou o ["Considerações sobre Cloud Storage Pools"](#).

Passos

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

A tabela Cloud Storage Pools lista os Cloud Storage Pools existentes.

2. Selecione a caixa de seleção do Cloud Storage Pool que você deseja editar e, em seguida, selecione **Ações > Editar**.

Como alternativa, selecione o nome do Cloud Storage Pool e, em seguida, selecione **Editar**.

3. Conforme necessário, altere o nome do Cloud Storage Pool, o service endpoint, as credenciais de autenticação ou o método de verificação do certificado.



Você não pode alterar o tipo de provedor, o bucket S3 ou o contêiner do Azure para um pool de storage em nuvem.

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

4. Selecione **Salvar**.

Ao salvar um Cloud Storage Pool, o StorageGRID valida se o bucket ou contêiner e o endpoint do serviço existem e se podem ser acessados usando as credenciais que você especificou.

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

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

Remover um Cloud Storage Pool no StorageGRID

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

Antes de começar

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

Se necessário, use o ILM para mover os dados do objeto

Se o Cloud Storage Pool que você deseja remover contiver dados de objetos, você deve usar o ILM para mover os dados para um local diferente. Por exemplo, você pode mover os dados para Storage Nodes em sua grid ou para um Cloud Storage Pool diferente.

Passos

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

Você não pode remover um pool de storage em nuvem se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento.

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

clonou.

Você pode usar um ou mais pools de storage ou um Cloud Storage Pool diferente.

6. Edite cada uma das regras que você clonou.

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

7. "[Criar uma nova política ILM](#)" e substitua cada uma das regras antigas por uma regra clonada.

8. Ative a nova política.

9. Aguarde até que o ILM remova os objetos do pool de storage em nuvem e os coloque no novo local.

Excluir pool de storage em nuvem

Quando o pool de storage em nuvem estiver vazio e não for usado em nenhuma regra do ILM, você pode excluí-lo.

Antes de começar

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

Ocorre um erro se você tentar remover um Cloud Storage Pool que contenha objetos. Consulte "[Solucione problemas em pools de storage em nuvem](#)".



Ao criar 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 tem o nome `x-ntap-sgws-cloud-pool-uuid`.

Passos

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

Solucione problemas de Cloud Storage Pools no StorageGRID

Use estas etapas de solução de problemas para ajudar a resolver erros que você possa encontrar ao criar, editar ou excluir um Cloud Storage Pool.

Determine se ocorreu um erro

StorageGRID realiza uma verificação de integridade simples em cada Cloud Storage Pool, 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 StorageGRID encontra um erro no endpoint, realiza uma verificação de integridade a cada minuto a partir de cada Storage Node. Quando o erro é resolvido, as verificações de integridade param. Se uma verificação de integridade detectar um problema, uma mensagem será exibida na coluna Last error da tabela Cloud Storage Pools na página Storage pools.

A tabela mostra o erro mais recente detectado para cada Cloud Storage Pool e indica há quanto tempo o erro

ocorreu.

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

Verifique se o erro foi resolvido

Após resolver quaisquer problemas subjacentes, você pode verificar se o erro foi solucionado. Na página Cloud Storage Pool, selecione o endpoint e selecione **Limpar erro**. Uma mensagem de confirmação indica que StorageGRID limpou o erro do Cloud Storage Pool.

Se o problema subjacente tiver sido resolvido, a mensagem de erro deixará de ser exibida. No entanto, se o problema subjacente não tiver sido corrigido (ou se ocorrer um erro diferente), a mensagem de erro será exibida na coluna "Último erro" dentro de alguns minutos.

Erro: a verificação de integridade falhou. Erro do endpoint.

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. Esse erro ocorre quando a operação PUT não possui um cabeçalho HTTP com um valor de checksum de carga, como Content-MD5. Esse valor de cabeçalho é exigido pela AWS para operações PUT em buckets com S3 Object Lock habilitado.

Para corrigir esse problema, siga os passos em ["Editar um pool de armazenamento em nuvem"](#) sem fazer nenhuma alteração. Essa ação aciona a validação da configuração do Cloud Storage Pool que detecta e atualiza automaticamente o sinalizador S3 Object Lock na configuração do endpoint 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 Cloud Storage Pool. Esse erro ocorre se o bucket ou contêiner incluir o arquivo marcador `x-ntap-sgws-cloud-pool-uuid`, mas esse arquivo não tiver 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 um destes passos para corrigir o problema:

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

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

- Se o ``x-ntap-sgws-cloud-pool-uuid`` arquivo for o único objeto no bucket, exclua esse 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 endpoint

Você pode encontrar esse erro nas seguintes circunstâncias:

- Quando você tenta criar ou editar um Cloud Storage Pool.
- Ao selecionar uma combinação de plataforma, autenticação ou protocolo não compatível com o S3 Object Lock durante a configuração de um novo Cloud Storage Pool. Consulte "[Considerações sobre pools de armazenamento em nuvem](#)".

Este erro indica que um problema de conectividade ou de configuração está impedindo 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 endpoint 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 Storage Nodes acessem o endpoint do serviço usado para o Cloud Storage Pool.
- Se o erro for devido a uma plataforma, autenticação ou protocolo não suportado, altere para uma configuração suportada com S3 Object Lock e tente salvar o novo Cloud Storage Pool novamente.
- Para todas as outras mensagens de erro do 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 que você especificou para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.

Erro: Falha ao analisar o certificado da CA

Você pode encontrar esse erro ao tentar criar ou editar um Cloud Storage Pool. O erro ocorre se StorageGRID não conseguir analisar o certificado inserido durante a configuração do Cloud Storage Pool.

Para corrigir o problema, verifique o certificado da Autoridade Certificadora (CA) que você forneceu para identificar possíveis problemas.

Erro: Não foi encontrado um Cloud Storage Pool com este ID

Você pode encontrar esse erro ao tentar editar ou excluir um Cloud Storage Pool. Esse erro ocorre se o endpoint retornar uma resposta 404, que pode significar uma das seguintes situações:

- 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 possui as permissões necessárias.
- Edite o Cloud Storage Pool com credenciais que possuam as permissões necessárias.
- Se as permissões estiverem corretas, entre em contato com o suporte.

Erro: Não foi possível verificar o conteúdo do Cloud Storage Pool. Erro do endpoint

Você pode encontrar esse erro ao tentar excluir um Cloud Storage Pool. Esse erro indica que algum problema de conectividade ou configuração está impedindo 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 Cloud Storage Pool. Você não pode excluir um Cloud Storage Pool se ele contiver dados que foram movidos para lá pelo ILM, dados que já estavam no bucket antes de você configurar o Cloud Storage Pool ou dados que foram colocados no bucket por outra fonte após a criação do Cloud Storage Pool.

Tente uma ou mais destas etapas para corrigir o problema:

- Siga as instruções para mover objetos de volta para StorageGRID em "Ciclo de vida de um objeto do Cloud Storage Pool".
- 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 Cloud Storage Pool 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 storage não transparente entre os Storage Nodes e o endpoint S3 externo usado para o Cloud Storage Pool. Esse erro ocorre se o servidor proxy externo não conseguir alcançar o endpoint do Cloud Storage Pool. Por exemplo, o servidor DNS pode não conseguir resolver o nome do host ou pode haver um problema de rede 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 storage.

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

Você pode encontrar esse erro ao tentar excluir um Cloud Storage Pool. Esse erro ocorre quando a autenticação exige um certificado X.509 para garantir que o Cloud Storage Pool externo correto seja validado e que o pool externo esteja vazio antes da exclusão da configuração do Cloud Storage Pool.

Tente seguir estes passos 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 Cloud Storage Pool seja resolvido.

Informações relacionadas

["Ciclo de vida de um objeto de cloud storage pool"](#)

Gerencie perfis de codificação de apagamento no StorageGRID

Você pode visualizar os detalhes de um perfil de codificação de apagamento e renomeá-lo, se necessário. Você pode desativar um perfil de codificação de apagamento caso ele não esteja sendo usado em nenhuma regra de gerenciamento do ciclo de vida das informações (ILM).

Antes de começar

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

Veja os detalhes do perfil de codificação de apagamento

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

Passos

1. Selecione **Configuração > Sistema > Codificação de apagamento**.
2. Selecione o perfil. A página de detalhes do perfil é exibida.
3. Opcionalmente, visualize a guia de regras do ILM para ver uma lista das regras do ILM que usam o perfil e das políticas do ILM que usam essas regras.
4. Opcionalmente, consulte a guia Nós de Armazenamento para obter detalhes sobre cada Nó de Armazenamento no pool de storage do perfil, como o site onde está localizado e o uso de storage.

Renomear um perfil de codificação de apagamento

Você pode querer renomear um perfil de codificação de apagamento para tornar mais óbvio o que o perfil faz.

Passos

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

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



Os nomes dos perfis de codificação de apagamento devem ser únicos. Ocorre um erro de validação 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 apagamento

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



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

Sobre esta tarefa

StorageGRID impede você de desativar um perfil de codificação de apagamento se alguma das seguintes condições for verdadeira:

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

Passos

1. Selecione **Configuração > Sistema > Codificação de apagamento**.
2. Na guia Ativo, verifique a coluna **Status** para confirmar que o perfil de codificação de apagamento que você deseja desativar não está sendo usado em nenhuma regra ILM.

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

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

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

Onde o perfil foi utilizado?	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 utilizado?	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 ILM afetadas. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de apagamento. ii. Continue com este procedimento.	"Trabalhe com regras e políticas do ILM"
Em uma regra ILM que está atualmente em uma política ILM ativa	i. Clone a política. ii. Remova a regra ILM que usa o perfil de erasure-coding. iii. Adicione uma ou mais novas regras ILM para garantir que os objetos estejam protegidos. iv. Salve, simule e ative a nova política. v. Aguarde a aplicação da nova política e a movimentação dos objetos existentes para novos locais com base nas novas regras que você adicionou. Nota: Dependendo do número de objetos e do tamanho do seu sistema StorageGRID, as operações do ILM podem levar semanas ou até meses para mover os objetos para novos locais, com base nas novas regras do ILM. Embora você possa tentar desativar com segurança um perfil de codificação de apagamento enquanto ele ainda estiver associado a dados, a operação de desativação falhará. Uma mensagem de erro informará você 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 apagamento. vii. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras e políticas do ILM"

Onde o perfil foi utilizado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que está atualmente em uma política ILM	i. Edite a política. ii. Remova a regra ILM que usa o perfil de erasure-coding. iii. Adicione uma ou mais novas regras 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 apagamento. vi. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras e políticas do ILM"

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

- 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 apagamento é exibida.



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

- Se você tem certeza de que deseja desativar o perfil, selecione **Desativar**.

Resultados

- Se StorageGRID conseguir desativar o perfil de codificação de apagamento, o status dele será "Desativado". Você não poderá mais selecionar esse perfil para nenhuma regra ILM. Você não pode reativar um perfil desativado.
- Se StorageGRID não conseguir desativar o perfil, uma mensagem de erro será exibida. Por exemplo, uma mensagem de erro será exibida se ainda houver dados de objeto associados a esse perfil. Pode ser necessário aguardar algumas semanas antes de tentar o processo de desativação novamente.

Configure regiões S3 para StorageGRID

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

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



Você não pode alterar a região de um bucket depois que o bucket foi criado.

Antes de começar

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

Sobre esta tarefa

Ao criar um bucket S3, você pode especificar que ele 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 a requisitos regulatórios.

Ao criar uma regra ILM, você pode querer usar a região associada a um bucket do S3 como um filtro avançado. Por exemplo, você pode criar uma regra que se aplique somente a objetos em buckets do S3 criados na `us-west-2` região. Em seguida, você pode especificar que cópias desses objetos sejam colocadas em Storage Nodes em um data center dentro dessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os buckets são considerados pertencentes à `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 API S3 PUT Bucket. Ocorrerá um erro se uma solicitação PUT Bucket usar uma região que não foi definida no StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket do S3. Os nomes de região diferenciam maiúsculas de minúsculas. Os caracteres válidos são números, letras e hífens.



EU não é considerado um sinônimo para `eu-west-1`. Se você quiser usar a região EU ou `eu-west-1`, deve usar o nome exato.

- Não é possível excluir ou modificar uma região se ela estiver sendo usada em uma regra atribuída a qualquer política (ativa ou inativa).
- Se você usar uma região inválida como filtro avançado em uma regra ILM, não poderá adicionar essa regra a uma política.

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

- Se você excluir uma região depois de usá-la para criar um bucket do S3, precisará adicioná-la novamente caso queira usar o filtro avançado de Location Constraint para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM > Regiões**.

A página Regiões é exibida.

2. Selecione a guia **Todas as regiões** ou **Região padrão**.

Todas as regiões

A aba **Todas as regiões** lista as regiões atualmente definidas, incluindo a região padrão definida.



Não é possível remover ou modificar a região padrão na guia **Todas as regiões**. Use a guia **Região padrão** para alterar a região padrão.

- Para adicionar uma região, selecione **Adicionar outra região**.
- Insira o nome de uma região que você deseja usar ao criar buckets do S3.

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

- Para remover uma região não utilizada, selecione o ícone de excluir

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

- 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. Consulte "[Utilize filtros avançados em regras ILM](#)".

Região padrão

A aba **Região padrão** exibe a região padrão definida atualmente, a qual você pode modificar.

- Para alterar a região padrão, selecione o nome da região nas opções disponíveis na lista suspensa **Default region**.
- Selecione **Salvar**.

Criar regra ILM

Saiba mais sobre as regras ILM no StorageGRID

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

Cada objeto inserido 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 StorageGRID executa para copiar e armazenar esse objeto.



Os metadados de objeto não são gerenciados pelas regras de ILM. Em vez disso, os metadados de objeto são armazenados em um banco de dados Cassandra, conhecido como repositório de metadados. Três cópias dos metadados de objeto são mantidas automaticamente em cada site para proteger os dados contra perda.

Elementos de uma regra ILM

Uma regra ILM possui 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, StorageGRID aplica a regra e cria 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 de objetos. Cada regra pode incluir uma sequência de instruções de posicionamento para alterar o número, o tipo e a localização das cópias de objetos ao longo do tempo. Quando o período de um posicionamento expira, as instruções do próximo posicionamento 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 durante a ingestão (quando um cliente S3 salva um objeto na grid).

Filtragem de regras ILM

Ao criar uma regra 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 (padrão) regra em uma política ILM. A regra padrão fornece instruções de storage para objetos que não correspondem aos filtros de outra regra.

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

Os filtros básicos oferecem uma maneira simples de aplicar regras diferentes a um grande número de objetos. Por exemplo, os registros financeiros da sua empresa podem precisar ser armazenados para atender a requisitos regulatórios, enquanto os dados do departamento de marketing podem precisar ser armazenados para facilitar as operações diárias. Depois de criar contas de locatário separadas para cada departamento ou depois de segregar os 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.

- Os filtros avançados oferecem controle preciso. Você pode criar filtros para selecionar objetos com base nas seguintes propriedades do objeto:
 - Tempo de ingestão
 - Último tempo de acesso
 - Todo ou parte do nome do objeto (chave)
 - Restrição de localização (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 raramente depois disso, enquanto objetos que contêm informações sobre consultas de pacientes podem precisar ser copiados para o departamento de faturamento na sede da rede de saúde. Você pode criar filtros que identificam 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 arquivos de imagem grandes de forma diferente dos registros de fornecedores, enquanto o departamento de Recursos Humanos pode precisar armazenar registros de pessoal em uma região geográfica específica e informações de políticas de forma centralizada. Nesse caso, você pode criar regras que filtrem 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 posicionamento se aplica a um único período de tempo.

Ao criar instruções de posicionamento:

- Você começa 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 não atual ou um tempo definido pelo usuário.
- Em seguida, você especifica quando o posicionamento será aplicado, em relação ao tempo de referência. Por exemplo, um posicionamento pode começar no dia 0 e continuar por 365 dias, em relação ao momento em que o objeto foi ingerido.
- Por fim, você especifica o tipo de cópias (replicação ou codificação de apagamento) e o local onde as cópias são armazenadas. Por exemplo, você pode querer armazenar duas cópias replicadas em dois locais diferentes.

Cada regra pode definir várias colocações para um único período de tempo e colocações diferentes para períodos de tempo diferentes.

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

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

Time period and placements Sort by start date

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

Time period 1
From Day 0 store for 365 days

Store objects by replicating 2 copies at Data Center 1 , Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

1

Add other type or location

Time period 2
From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

2

Add other type or location

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

- A primeira linha cria duas cópias replicadas do objeto em dois sites de data center.
- A segunda linha cria uma cópia 6+3 com codificação de apagamento usando todos os sites do data center.

A segunda instrução de colocação **2** cria duas cópias após um ano e guarda essas cópias 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 lacunas entre os períodos de tempo que você definiu e que a instrução de posicionamento final continue indefinidamente ou até que você não precise mais de nenhuma cópia de objeto.

À medida que cada período de tempo definido na 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 da regra ILM

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

- **Balanceado:** StorageGRID tenta criar todas as cópias especificadas na regra ILM durante a ingestão; se isso não for possível, cópias intermediárias são criadas e uma mensagem de sucesso é retornada ao cliente. As cópias especificadas na regra ILM são criadas sempre que possível.
- **Estrito:** Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.
- **Confirmação dupla:** StorageGRID cria imediatamente cópias provisórias do objeto e retorna sucesso ao

cliente. As cópias especificadas na regra ILM são criadas sempre que possível.

Informações relacionadas

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

Exemplo de regra ILM

Por exemplo, uma regra ILM poderia especificar o seguinte:

- Aplica-se somente aos objetos pertencentes ao Tenant A.
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um site diferente.
- As duas cópias serão mantidas "para sempre", o que significa que StorageGRID não as excluirá automaticamente. Em vez disso, StorageGRID reterá esses objetos até que sejam excluídos por uma solicitação de exclusão do cliente ou pelo término do ciclo de vida do bucket.
- Use a opção Balanceada para o comportamento de ingestão: a instrução de posicionamento em dois sites é aplicada assim que o Tenant 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 Tenant A salvar um objeto, StorageGRID fará duas cópias provisórias nos Storage Nodes do Site 1. Assim que o Site 2 estiver disponível, StorageGRID fará a cópia necessária nesse site.

Informações relacionadas

- ["O que é um pool de storage"](#)
- ["O que é um pool de storage em nuvem"](#)

Acesse o assistente Criar uma regra ILM no StorageGRID

As regras do ILM permitem gerenciar a alocação de dados de objetos ao longo do tempo. Para criar uma regra do ILM, você utiliza o assistente Criar uma regra do ILM.



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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Se você deseja especificar a quais contas de locatário essa regra se aplica, você tem o ["Permissão de contas de tenant"](#) ou conhece o ID da conta para cada conta.
- Se você deseja que a regra filtre objetos com base nos metadados de tempo de acesso, as atualizações de tempo de acesso devem estar habilitadas pelo bucket do S3.
- Você configurou todos os Cloud Storage Pools que planeja usar. Consulte ["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 já está familiarizado

com o ["Requisitos para S3 Object Lock"](#).

- Opcionalmente, você assistiu ao vídeo:

[Visão geral das regras do ILM](#)

Sobre esta tarefa

Ao criar regras ILM:

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

Passos

1. Selecione **ILM > Regras**.
2. Selecione **Criar**. ["Etapa 1 \(Inserir detalhes\)"](#)A tela do assistente Criar uma regra ILM é exibida.

Inserir detalhes e filtros para uma regra ILM do StorageGRID

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 é opcional.

Sobre esta tarefa

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

Passos

1. Insira 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 que possa reconhecê-la posteriormente.

3. Opcionalmente, selecione uma ou mais contas de locatário do S3 às quais esta regra se aplica. Se esta regra se aplica a todos os locatários, deixe este campo em branco.

Se você não tiver a permissão de acesso Root ou a permissão de Tenant accounts, não poderá selecionar locatários da lista. Em vez disso, insira o ID do locatário ou vários IDs como uma sequência separada por vírgulas.

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

Se a opção **aplica a todos os buckets** estiver selecionada (padrão), a regra se aplica a todos os buckets

S3.

5. Para tenants do S3, selecione opcionalmente **Sim** para aplicar a regra somente a versões de objetos mais antigas em buckets do S3 que tenham versionamento ativado.

Se você selecionar **Sim**, "Hora não atual" será selecionada automaticamente para Hora de referência em ["Etapa 2 do assistente Criar uma regra ILM"](#).



O tempo não atual aplica-se apenas a objetos S3 em buckets com versionamento ativado. Consulte ["Operações em buckets, PutBucketVersioning"](#) e ["Gerencie objetos com S3 Object Lock"](#).

Você pode usar essa opção para reduzir o impacto de storage de objetos versionados filtrando versões de objetos não atuais. Consulte ["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 se aplica a todos os objetos que correspondem aos filtros básicos. Para mais informações sobre filtragem avançada, consulte [Utilize filtros avançados em regras ILM](#) e [Especifique vários tipos de metadados e valores](#).

7. Selecione **Continuar**. ["Etapa 2 \(Definir colocações\)"](#) O assistente Criar uma regra ILM será exibido.

Utilize filtros avançados em regras ILM

A filtragem avançada permite que você crie regras ILM que se aplicam somente a objetos específicos com base em seus metadados. Ao configurar a filtragem avançada para uma regra, você seleciona o tipo de metadado que deseja corresponder, seleciona um operador e especifica um valor de metadado. Quando os objetos são avaliados, a regra ILM é aplicada somente àqueles objetos que possuem metadados que correspondem 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 • é em ou antes de • é depois • é em ou após	Data e hora em que o objeto foi ingerido. Nota: Para evitar problemas de recursos ao ativar uma nova política 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" para um valor maior ou igual ao horário aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.

Tipo de metadados	Operadores suportados	Valor de metadados
Chave	• igual a • não é igual • contém • não contém • começa com • não começa com • termina com • não termina com	Toda ou parte de uma chave de objeto S3 exclusiva. Por exemplo, você pode querer encontrar objetos que terminem com <code>.txt</code> ou comecem com <code>test-object/</code>.
Último tempo de acesso	• é • não é • é antes • é em ou antes de • é depois • é em ou após	Data e hora em que o objeto foi recuperado (lido ou visualizado) pela última vez. Observação: Se você planeja "usar o último tempo de acesso" como um filtro avançado, as atualizações do tempo de acesso mais recente devem estar ativadas para o bucket do S3.
Restrição de localização (somente S3)	• igual a • não é igual	A região onde um bucket do S3 foi criado. Use ILM > Regiões para definir as regiões que são exibidas. Nota: O valor <code>us-east-1</code> corresponderá a objetos em buckets criados na região <code>us-east-1</code>, bem como a objetos em buckets que não têm região especificada. Consulte "Configurar regiões S3".
Tamanho do objeto	• igual a • não é igual • menor que • menor ou igual a • maior que • maior ou igual a	O tamanho do objeto. A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

Tipo de metadados	Operadores suportados	Valor de metadados
Metadados do usuário	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • 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 do usuário de <code>color=blue</code>, especifique <code>color</code> para Nome dos metadados do usuário, <code>equals</code> para o operador e <code>blue</code> para Valor dos metadados. Observação: Os nomes dos metadados do usuário não diferenciam maiúsculas de minúsculas; os valores dos metadados do usuário diferenciam maiúsculas de minúsculas.
Tag de objeto (somente S3)	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • 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 <code>Image=True</code>, especifique <code>Image</code> para Nome da tag de objeto, <code>equals</code> para o operador e <code>True</code> para Valor da tag de objeto. Observação: Os nomes e valores das tags de objeto diferenciam maiúsculas de minúsculas. Você deve inserir esses itens exatamente como foram definidos para o objeto.

Especifique vários tipos de metadados e valores

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 com tamanho entre 10 MB e 100 MB, você selecionaria o tipo de metadado **Object size** e especificaria dois valores de metadados.

- O primeiro valor de metadados especifica objetos com tamanho igual ou superior a 10 MB.
- O segundo valor de metadados especifica objetos com tamanho igual ou inferior a 100 MB.

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

Object size
greater than or equal to
10
MB

and
Object size
less than or equal to
100
MB

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

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

User metadata camera_type equals Brand A

[Add another advanced filter](#)

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

User metadata camera_type equals Brand B

and Object size less than or equal to 10 MB

[Add another advanced filter](#)

Defina as instruções de posicionamento para uma regra ILM do StorageGRID

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



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

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de posicionamento. Cada instrução de posicionamento 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 indefinidamente 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 de apagamento 2+1 é criada e salva em apenas um site.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Passos

1. Em **Horário de referência**, selecione o tipo de horário 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 tempo de acesso	O momento em que o objeto foi recuperado (lido ou visualizado) pela última vez. Para usar esta opção, as atualizações de tempo de acesso devem estar habilitadas para o bucket S3. Consulte "Usar tempo de acesso nas regras do ILM".
Tempo de criação definido pelo usuário	Um horário especificado nos metadados definidos pelo usuário.
Tempo não atual	A opção "Tempo não atual" é selecionada automaticamente se você selecionou Sim para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" em "Etapa 1 do assistente Criar uma regra ILM" .

Se você deseja criar uma regra *em conformidade*, você deve selecionar **Horário de ingestão**. Consulte ["Gerencie objetos com S3 Object Lock"](#).

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

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 deseja criar cópias replicadas:
 - a. Na lista suspensa **Armazenar objetos por**, selecione **replicating**.
 - b. Selecione o número de cópias que você deseja fazer.

Um aviso é exibido se você alterar o número de cópias para 1. Uma regra 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:

- Aumente o número de cópias para o período de tempo.
- Adicione cópias a outros pools de storage ou a um Cloud Storage Pool.
- Selecione **codificação de apagamento** 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 storage que você deseja adicionar.

Se você especificar apenas um pool de storage, esteja ciente de que StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer Storage Node. Se sua grid incluir três Storage Nodes e você selecionar 4 como o número de cópias, apenas três cópias serão criadas—uma cópia para cada Storage Node.

O alerta **Implantação do ILM inviável** é acionado para indicar que a regra do ILM não pôde ser completamente aplicada.

Se você especificar mais de um pool de storage, lembre-se destas regras:

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

4. Se você deseja criar uma cópia com codificação de apagamento:

- a. Na lista suspensa **Armazenar objetos por**, selecione **erasure coding**.



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

- 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 de **Tamanho do objeto** para qualquer valor maior que 200 KB.
 - c. Selecione o pool de storage que você deseja adicionar e o esquema de codificação de apagamento

que você deseja usar.

O local de armazenamento de uma cópia com codificação de apagamento inclui o nome do esquema de codificação de apagamento, seguido pelo nome do pool de storage.

Os esquemas de codificação de apagamento disponíveis são limitados pelo número de Storage Nodes no pool de storage que você selecionar. Um **Recommended** badge aparece ao lado dos esquemas que fornecem o "[melhor proteção ou menor sobrecarga de storage](#)".

5. Opcionalmente:

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



A exclusão de objetos ocorre com base nas seguintes configurações:

- Os objetos são excluídos automaticamente ao final do último período, a menos que outro período termine com **forever**.
- Dependendo de "[Configurações de período de retenção de bucket e tenant](#)", os objetos podem não ser excluídos mesmo que o período de retenção termine.

6. Se você deseja armazenar objetos em um pool de Cloud Storage:

- a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.
- b. Selecione o campo **cópias em** e, em seguida, selecione um Cloud Storage Pool.

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

- Não é possível selecionar mais de um Cloud Storage Pool em uma única instrução de posicionamento. Da mesma forma, não é possível selecionar um Cloud Storage Pool e um pool de storage na mesma instrução de posicionamento.
- Você só pode armazenar uma cópia de um objeto em qualquer pool de storage do Cloud Storage. Uma mensagem de erro aparece se você definir **Cópias** para 2 ou mais.
- Não é possível armazenar mais de uma cópia de um objeto em qualquer Cloud Storage Pool ao mesmo tempo. Uma mensagem de erro aparece se vários posicionamentos que usam um Cloud Storage Pool tiverem datas sobrepostas ou se várias linhas no mesmo posicionamento usarem um Cloud Storage Pool.
- Você pode armazenar um objeto em um Cloud Storage Pool ao mesmo tempo em que esse objeto está sendo armazenado como cópias replicadas ou codificadas por codificação de apagamento no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de posicionamento para o período, para que possa especificar o número e os tipos de cópias para cada local.

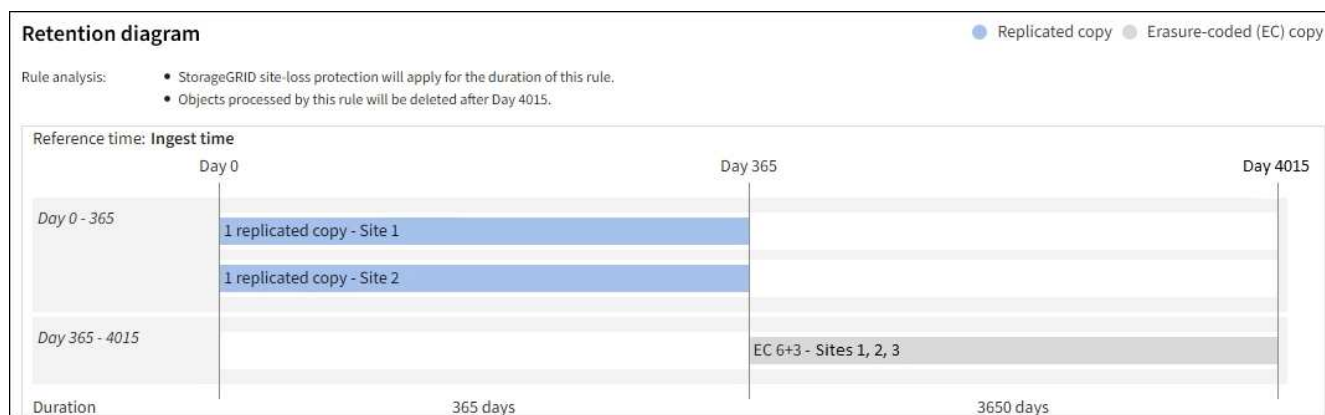
7. No diagrama de retenção, confirme suas instruções de posicionamento.

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 de codificação de apagamento 6+3 será salva em três sites. Após um total de 11 anos, os objetos serão excluídos do StorageGRID.

A seção de 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 sites."](#)



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

Use tempo de acesso nas regras do StorageGRID ILM

Você pode usar tempo de acesso como referência em uma regra do ILM. Por exemplo, você pode querer manter os objetos visualizados nos últimos três meses em Storage Nodes locais, enquanto move os objetos que não foram visualizados recentemente para um local externo. Você também pode usar tempo de acesso como um filtro avançado se quiser que uma regra do ILM se aplique somente aos objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

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

- Ao usar tempo de acesso como referência, esteja ciente de que alterar o tempo 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 acesso ao objeto.

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

- Ao usar tempo de acesso como filtro avançado ou como horário de referência, você deve habilitar as atualizações do tempo de acesso para buckets S3. Você pode usar o ["Tenant Manager"](#) ou o ["API de gerenciamento de inquilinos"](#).



As atualizações de tempo de acesso estão desativadas por padrão para buckets do S3.



Tenha em mente que habilitar as atualizações do tempo de acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impacto no desempenho ocorre porque StorageGRID precisa atualizar os objetos com novos registros de data e hora sempre que eles são recuperados.

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

Tipo de solicitação	Se o tempo de acesso é atualizado quando as atualizações do tempo de acesso estão desativadas	Se o tempo de acesso é atualizado quando as atualizações do tempo de acesso estão ativadas
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Sim
Solicitação para atualizar os metadados de um objeto	Sim	Sim
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia original • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Solicitação para concluir um upload multipart	Sim, para o objeto montado	Sim, para o objeto montado

Selecione o comportamento de ingestão para uma regra ILM do StorageGRID

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

Sobre esta tarefa

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

Passos

1. Selecione a opção **"comportamento de ingestão"** para usar.

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



Você não pode usar a opção Equilibrado ou Rigoroso se a regra usar um destes posicionamentos:

- Um pool de storage em nuvem no dia 0
- Um pool de storage em nuvem quando a regra usa um horário de criação definido pelo usuário como horário de referência

Consulte **"Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"**.

2. Selecione **Create**.

A regra ILM é criada. A regra só entra em vigor depois de ser adicionada a uma **"Política ILM"** e essa política ser ativada.

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

Crie uma regra ILM padrão no StorageGRID

Antes de criar uma política ILM, você deve criar uma regra padrão para incluir na política quaisquer objetos que não correspondam a nenhuma outra regra. A regra padrão não pode usar nenhum filtro. Ela deve se aplicar a todos os tenants, todos os buckets e todas as versões de objeto.

Antes de começar

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

Sobre esta tarefa

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

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

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

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

Select rules

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

Ao criar a regra padrão, tenha em mente os seguintes requisitos:

- A regra padrão será automaticamente inserida como a última regra quando você a adicionar 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 utilize uma regra que crie cópias codificadas por apagamento como regra padrão de uma política. As regras de codificação por apagamento devem usar um filtro avançado para impedir que objetos menores sejam codificados por apagamento.

- Em geral, a regra padrão deve manter os objetos indefinidamente.
- Se você estiver usando (ou planeja habilitar) a configuração global de S3 Object Lock, a regra padrão deve estar em conformidade.

Passos

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

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

3. Insira um nome exclusivo para a regra no campo **Rule name**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.
5. Deixe o campo **Tenant accounts** em branco.

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

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

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

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

A regra padrão não pode especificar nenhum filtro.

9. Selecione **Next**.

A etapa 2 (Definir posicionamentos) é exibida.

10. Para o horário de referência, selecione qualquer opção.

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

11. Especifique as instruções de posicionamento para a regra padrão.
 - A regra padrão deve reter os objetos indefinidamente. Um aviso será exibido ao ativar uma nova política se a regra padrão não reter os objetos indefinidamente. Você deve confirmar se esse é o comportamento que você espera.
 - A regra padrão deve criar cópias replicadas.



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

- Se você estiver usando (ou planeja habilitar) a configuração global S3 Object Lock, a regra padrão deve ser compatível:
 - É necessário criar pelo menos duas cópias replicadas do objeto ou uma cópia com código de apagamento.
 - Essas cópias devem existir nos Storage Nodes durante toda a duração de cada linha nas instruções de posicionamento.
 - Não é possível salvar cópias de objetos em um Cloud Storage Pool.
 - Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando o horário de ingestão como horário de referência.
 - Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

12. Consulte o diagrama de retenção para confirmar suas instruções de posicionamento.

13. Selecione **Continue**.

A etapa 3 (Selecionar comportamento de ingestão) aparece.

14. Selecione a opção de ingestão que você deseja usar e selecione **Criar**.

Gerenciar políticas ILM

Saiba mais sobre as políticas ILM no StorageGRID

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



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

Política ILM padrão

Ao instalar StorageGRID e adicionar sites, uma política ILM padrão é criada automaticamente, da seguinte forma:

- Se sua grade contiver um único site, a política padrão contém uma regra padrão que replica duas cópias de cada objeto nesse site.
- Se a sua grid contiver mais de um site, a regra padrão replica uma cópia de cada objeto em cada site.

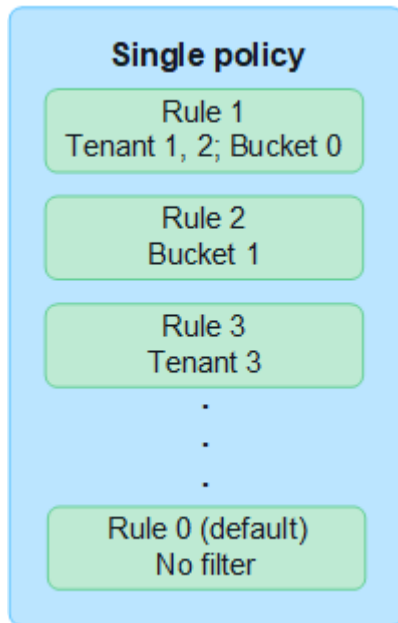
Se a política padrão não atender aos seus requisitos de armazenamento, você pode criar suas próprias regras e políticas. Consulte ["Crie uma regra ILM"](#) e ["Crie uma política ILM"](#).

Uma ou várias políticas ILM ativas?

Você pode ter uma ou mais políticas ILM ativas simultaneamente.

Uma política

Se sua grid usar um esquema de proteção de dados simples, com poucas regras específicas para tenants e buckets, utilize uma única política ILM ativa. As regras ILM podem conter filtros para gerenciar diferentes buckets ou tenants.



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

Várias políticas

Para oferecer diferentes opções de qualidade de serviço aos clientes, você pode ter mais de uma política ativa simultaneamente. Cada política pode gerenciar clientes, buckets do S3 e objetos específicos. Ao aplicar ou alterar uma política para um conjunto específico de clientes ou objetos, as políticas aplicadas a outros clientes e objetos não são afetadas.

Etiquetas de política ILM

Se você deseja permitir que os locatários alternem facilmente entre várias políticas de proteção de dados por bucket, use várias políticas ILM com *tags de política ILM*. Você atribui cada política ILM a uma tag, então os locatários adicionam uma tag a um bucket para aplicar a política a esse bucket. Você só pode definir tags de política ILM em buckets S3.

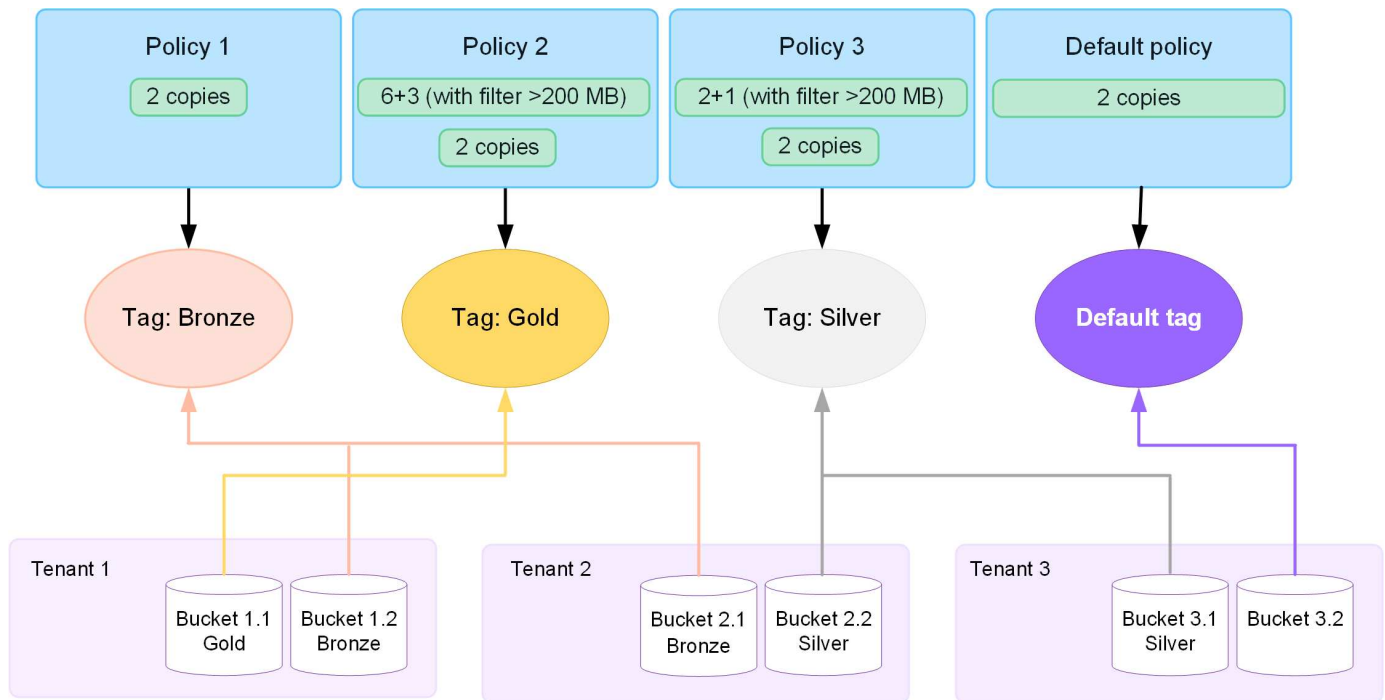
Por exemplo, você pode ter três tags chamadas Gold, Silver e Bronze. Você pode atribuir uma política ILM a cada tag, com base em quanto tempo e onde essa política armazena objetos. Os tenants podem escolher qual política usar marcando seus buckets. Um bucket com a tag Gold é gerenciado pela política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



Você pode "[Crie no máximo 10 tags de política](#)" para sua grid.

Tag de política ILM padrão

Uma tag de política ILM padrão é criada automaticamente quando você instala StorageGRID. Cada grid deve ter uma política ativa atribuída à tag Default. A política padrão se aplica a qualquer bucket S3 sem tag.



Como uma política ILM avalia objetos?

Uma política ILM ativa controla a localização, 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 ILM na política, da seguinte forma:

1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto é 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 é 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 se aplicar 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 ILM

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

• Regra 1: Cópias replicadas para Tenant A

- Associe todos os objetos pertencentes ao Tenant A.
- Armazene esses objetos como três cópias replicadas em três sites.
- Os objetos pertencentes a outros tenants não correspondem à Regra 1, portanto, são avaliados de acordo com a Regra 2.

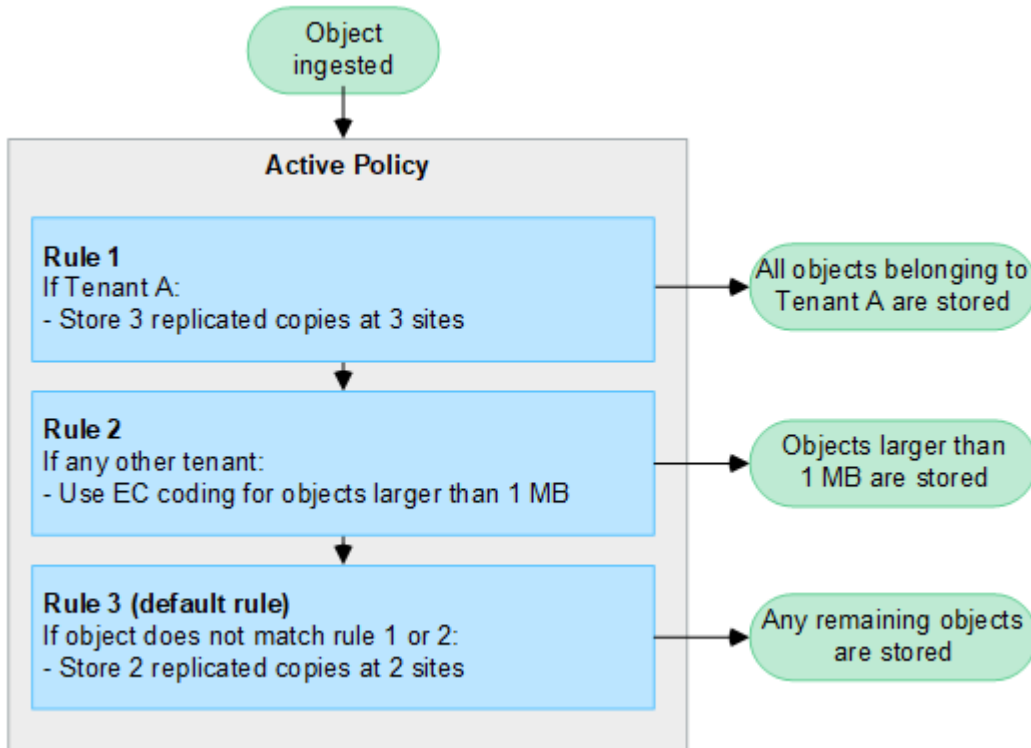
• Regra 2: codificação de apagamento para objetos maiores que 1 MB

- 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 apagamento 6+3 em três sites.

- Não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados de acordo com a Regra 3.

- **Regra 3: 2 cópias 2 centros de dados** (padrão)

- É a última e padrão regra na política. Não utiliza filtros.
- Faça duas cópias replicadas de todos os objetos que não correspondem à Regra 1 ou à Regra 2 (objetos que não pertencem ao Tenant A e que têm 1 MB ou menos).



O que são políticas ativas e inativas?

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

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

Ao ativar uma política ILM, 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 ILM da nova política são implementadas.

Se você ativar mais de uma política ILM simultaneamente 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 criar uma política de ILM

- Utilize apenas a política fornecida pelo sistema, *Baseline 2 copies policy*, em sistemas de teste. Para StorageGRID 11.6 e versões anteriores, a regra *Make 2 Copies* nesta política utiliza o pool de storage *All*

Storage Nodes, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto podem ser colocadas no mesmo site.



O pool de storage 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 All Storage Nodes ainda existirá. Se você instalar StorageGRID 11.7 ou posterior como uma nova instalação, o pool All Storage Nodes não será criado.

- Ao criar uma nova política, considere todos os diferentes tipos de objetos que podem ser inseridos em sua grid. Certifique-se de que a política inclua regras para identificar e posicionar esses objetos conforme necessário.
- Mantenha a política ILM o mais simples possível. Isso evita situações potencialmente perigosas em que os dados dos objetos não são protegidos conforme o esperado quando alterações são feitas no sistema StorageGRID ao longo do tempo.
- Certifique-se de que as regras na política estejam na ordem correta. Quando a política é ativada, os objetos novos e existentes são avaliados pelas regras na ordem em que são listadas, começando do 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 ILM é a regra ILM padrão, que não pode usar nenhum filtro. Se um objeto não for correspondido por outra regra, a regra padrão controla onde esse objeto é colocado e por quanto tempo ele é retido.
- Antes de ativar uma nova política, revise 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.

Crie políticas ILM no StorageGRID

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

Ter uma política ILM ativa permite aplicar as mesmas regras ILM a todos os tenants e buckets.

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

Crie uma política ILM

Sobre esta tarefa

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



Utilize apenas as políticas fornecidas pelo sistema, 2 copies Policy (para grids de um único site) ou 1 Copy per Site (para grids de múltiplos sites), em sistemas de teste. Para StorageGRID 11.6 e versões anteriores, a regra padrão nesta política utiliza o pool de storage All Storage Nodes, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto podem ser colocadas no mesmo site.



Se o ["A configuração global de bloqueio de objeto S3 foi ativada"](#), você deve garantir que a política ILM esteja em conformidade com os requisitos dos buckets que têm S3 Object Lock ativado. Nesta seção, siga as instruções que mencionam ter S3 Object Lock ativado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "permissões de acesso necessárias".
- Você tem "regras ILM criadas" dependendo se o S3 Object Lock está ativado.

Bloqueio de objeto S3 não ativado

- Você tem "criou as regras ILM" que 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 ativado

- O "A configuração global de S3 Object Lock já está ativada" para o sistema StorageGRID.
- Você tem "criou as regras ILM compatíveis e não compatíveis" que 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:

Visão geral das políticas do ILM

Veja também "Use políticas ILM".

Passos

1. Selecione **ILM > Políticas**.

Se a configuração global de S3 Object Lock estiver ativada, a página de políticas do ILM indica quais regras do ILM estão em conformidade.

2. Determine como você deseja criar a política ILM.

Criar nova política

- a. Selecione **Criar policy**.

Clonar política existente

- a. Selecione a caixa de seleção da política com a qual você deseja começar e, em seguida, selecione **Clonar**.

Editar política existente

- a. Se uma política estiver inativa, você pode editá-la. Selecione a caixa de seleção da política inativa que você deseja começar, depois selecione **Editar**.

3. No campo **Policy name**, insira um nome exclusivo para a policy.
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 o nome de uma regra para visualizar as configurações dessa regra.

Se você estiver clonando uma política:

- As regras utilizadas pela política que você está clonando estão selecionadas.
- Se a política que você está clonando utilizava alguma regra sem filtros que não fosse a regra padrão, você será solicitado a remover todas as regras, exceto uma.
- Se a regra padrão utilizava um filtro, você será solicitado a selecionar uma nova regra padrão.
- Se a regra padrão não for a última regra, você pode movê-la para o final da nova política.

Bloqueio de objeto S3 não ativado

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



Não utilize a regra "Make 2 Copies" como regra padrão para uma política. A regra "Make 2 Copies" utiliza um único pool de storage, All Storage Nodes, 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 ativado

- 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 estão em conformidade e não utilizam nenhum filtro.



Não utilize a regra "Make 2 Copies" como regra padrão para uma política. A regra "Make 2 Copies" utiliza um único pool de storage, All Storage Nodes, que contém todos os sites. Se você utilizar essa regra, várias cópias de um objeto podem 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 têm S3 Object Lock ativado.



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

Veja também ["Exemplo 7: política ILM compatível para S3 Object Lock"](#).

6. Quando você terminar de selecionar a regra padrão, selecione **Continuar**.
7. Na etapa Outras regras, selecione quaisquer outras regras que você queira adicionar à política. Essas

regras usam pelo menos um filtro (conta de locatário, nome do bucket, filtro avançado ou o horário 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 S3 Object Lock estiver ativado e você também tiver selecionado uma regra "default" não compatível, essa regra será adicionada como a penúltima regra na política.



Um aviso será exibido se alguma regra não reter objetos indefinidamente. Ao ativar essa política, você deve confirmar que deseja que StorageGRID exclua os objetos quando as instruções de posicionamento da regra padrão expirarem (a menos que um ciclo de vida de 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.

Não é possível mover a regra padrão. Se o S3 Object Lock estiver ativado, você também não pode mover a regra "default" não compatível, caso uma tenha sido selecionada.



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

9. Se necessário, selecione **Selecionar regras** para adicionar ou remover regras.

10. Quando terminar, selecione **Salvar**.

11. Repita esses passos para criar políticas ILM adicionais.

12. **Simule uma política ILM**. É sempre recomendável simular uma política antes de ativá-la para garantir que ela funcione conforme o esperado.

Simule uma política

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

Antes de começar

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

Passos

1. Utilizando um cliente S3 ou o "[Console S3](#)", ingira os objetos necessários para testar cada regra.
2. Na página de políticas do ILM, selecione a caixa de seleção da política e depois 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 versionamento do S3 estiver ativado, insira opcionalmente um ID de versão para o objeto no campo **Version ID**.
5. Selecione **Simular**.
6. Na seção Resultados da Simulação, confirme que cada objeto foi correspondido pela regra correta.
7. Para determinar qual pool de storage ou perfil de codificação de apagamento está em vigor, selecione o nome da regra correspondente para acessar a página de detalhes da regra.



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

Resultados

Quaisquer alterações nas regras da política serão refletidas nos resultados da simulação e mostrarão a nova correspondência e a correspondência anterior. A janela "Simular política" mantém os objetos testados até que você selecione "Limpar tudo" ou o ícone de remoção  para cada objeto na lista de resultados da simulação.

Informações relacionadas

["Exemplos de simulações de políticas ILM"](#)

Ativar uma política

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

Antes de ativar uma nova política:

1. Simule a política para confirmar que ela se comporta conforme você espera.
2. Analise quaisquer alterações no posicionamento de objetos replicados e codificados para apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos forem avaliados e implementados.



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

Sobre esta tarefa

Ao ativar uma política 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 grid 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 grid não sejam removidos acidentalmente. Especificamente:

- Se você fizer alterações de política que **auumentem 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 dos 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 grid 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 Active policy, mas não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

Siga os passos para ativar uma ou mais políticas:

Ativar uma política

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

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

Alternativamente, você pode ativar uma única política na página **ILM > Policy tags**.

2. Na guia Políticas, selecione a caixa de seleção da política que você deseja ativar e, em seguida, selecione **Ativar**.
3. Siga a etapa apropriada:
 - Se uma mensagem de aviso solicitar que você confirme que deseja ativar a política, selecione **OK**.
 - Se aparecer uma mensagem de aviso contendo detalhes sobre a política:
 - i. Analise os detalhes para garantir que a política gerencie 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 armazenar objetos indefinidamente, mas uma ou mais outras regras tiverem retenção limitada, digite **sim** na caixa de texto.
 - iv. Selecione **Ativar política**.

Ativar várias políticas

Para ativar várias políticas, você deve criar etiquetas de política e atribuir uma política a cada etiqueta. Você pode criar no máximo 10 etiquetas de política para sua grid.



Quando várias tags de política estão em uso, se os tenants reatribuírem tags de política aos buckets com frequência, o desempenho do grid pode ser afetado. Se você tiver tenants não confiáveis, considere usar apenas a tag de política Default.

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



Os nomes e descrições das tags são visíveis para os locatários. Escolha valores que ajudem os locatários 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 ILM, use o menu suspenso para selecionar uma política para atribuir à tag.
6. Se aparecerem avisos na coluna Limitações da política, selecione **Exibir detalhes da política** para revisar a política.
7. Garanta que cada política gerencie os dados conforme o esperado.

8. Selecione **Ativar políticas atribuídas**. Ou selecione **Limpar alterações** para remover a atribuição da política.
9. Na caixa de diálogo Ativar políticas com novas tags, revise as descrições de como cada tag, política e regra gerenciará os 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, depois selecione **Ativar políticas**.

Informações relacionadas

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

Exemplo de simulações de políticas ILM no StorageGRID

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

Exemplo 1: verificar regras ao simular uma política ILM

Este exemplo descreve como verificar regras ao simular uma política.

Neste exemplo, a **Example ILM policy** está sendo simulada em relação aos objetos ingeridos em dois buckets. A política inclui três regras, conforme descrito a seguir:

- A primeira regra, **Duas cópias, dois anos para bucket-a**, aplica-se apenas aos objetos em bucket-a.
- A segunda regra, **Objetos EC > 1 MB**, aplica-se a todos os buckets, mas filtra objetos maiores que 1 MB.
- A terceira regra, **Duas cópias, dois data centers**, é a regra padrão. Ela não inclui nenhum filtro e não usa o Noncurrent reference time.

Após simular a política, confirme que cada objeto foi correspondido pela regra correta.

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

Neste exemplo:

- bucket-a/bucket-a object.pdf`correspondeu corretamente à primeira regra, que filtra objetos em `bucket-a.

- bucket-b/test object greater than 1 MB.pdf está em bucket-b, portanto não correspondeu à primeira regra. Em vez disso, foi corretamente correspondido pela segunda regra, que filtra objetos maiores que 1 MB.
- `bucket-b/test object less than 1 MB.pdf` Não correspondeu aos filtros das duas primeiras regras, portanto, será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: reordenar regras ao simular uma política ILM

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

Neste exemplo, a política **Demo** está sendo simulada. Essa política, que tem como objetivo encontrar objetos que possuam metadados de usuário `series=x-men`, inclui três regras, conforme descrito a seguir:

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

Passos

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

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

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

No entanto, `Havok.png` o objetivo era testar a regra dos **X-men**.

3. Para resolver o problema, reordene as regras.
 - a. Selecione **Concluir** para fechar a janela Simular Política 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 que você testou anteriormente são reavaliados em relação à política atualizada e os novos resultados da simulação são exibidos. No exemplo, a coluna "Regra correspondente" mostra que o `Havok.png` objeto agora corresponde à regra de metadados X-men, como esperado. A coluna "Correspondência anterior" mostra que a regra PNGs correspondeu ao objeto na simulação anterior.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X

Exemplo 3: corrigir uma regra ao simular uma política 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. Essa política tem como objetivo encontrar objetos que possuam `series=x-men` metadados de usuário. No entanto, resultados inesperados ocorreram ao simular essa política no objeto `Beast.jpg`. Em vez de corresponder à regra de metadados X-men, o objeto correspondeu à regra padrão, duas cópias dois data centers.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Quando um objeto de teste não 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. Analise a conta do locatário da regra, o horário de referência e os critérios de filtragem.

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

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

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

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	✕

Gerencie tags de política ILM no StorageGRID

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

Antes de começar

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

Veja os detalhes da tag de política 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 ILM



Os nomes e descrições das tags são visíveis para os locatários. Escolha valores que ajudem os locatários 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 etiqueta existente:

1. Selecione **ILM > Tags de política**.
2. Selecione a caixa de seleção da tag e, em seguida, 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 a tag de política ILM

Ao remover uma etiqueta de política, todos os buckets atribuídos a essa etiqueta terão a política Default aplicada.

Para remover uma tag:

1. Selecione **ILM > Tags de política**.
2. Selecione a caixa de seleção da tag e, em seguida, selecione **Remover**. Uma caixa de diálogo de confirmação aparece.

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

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

Informações relacionadas

["Saiba mais sobre como criar tags de política ILM"](#)

Verifique uma política ILM com pesquisa de metadados de objeto no StorageGRID

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

Antes de começar

Você possui um identificador de objeto, que pode ser um dos seguintes:

- **UUID:** O Identificador Universalmente Único do objeto.
- **CBID:** O identificador único do objeto no StorageGRID. Você pode obter o CBID de um objeto no log de auditoria. Insira o CBID em letras maiúsculas.
- **Bucket S3 e chave do objeto:** Quando um objeto é ingerido através da interface S3, o aplicativo cliente usa uma combinação de bucket e chave do objeto para armazenar e identificar o objeto. Se o bucket S3 for versionado e você quiser consultar uma versão específica de um objeto S3 usando o bucket e a chave do objeto, você terá o **ID da versão**.

Passos

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

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

- 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 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 com código de apagamento, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, a localização do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, é exibida uma lista dos segmentos do objeto, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os 100 primeiros segmentos são mostrados.
- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não têm garantia de persistência entre versões.

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

Se a opção de auditoria estiver habilitada, você também pode monitorar o log de auditoria para a mensagem ORLM Object Rules Met. 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 correção do posicionamento dos dados do objeto ou a integridade da política do ILM. Você deve avaliar isso por conta própria. Para obter detalhes, consulte ["Analisar registros de auditoria"](#).

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



A seguinte captura de tela é um exemplo. Seus resultados podem variar dependendo da sua 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": {
      "PAIIS": "2",

```

Informações relacionadas

["Utilize a API REST S3"](#)

Trabalhe com políticas ILM e regras ILM no StorageGRID

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

Antes de começar

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

Ver políticas do ILM

Para visualizar as políticas ILM ativas e inativas e o histórico de ativação das 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 das datas de início e término da ativação das políticas.
4. Selecione o nome de uma política para ver os detalhes da política.



Ao visualizar os detalhes de uma policy cujo status é Edited ou Deleted, uma mensagem aparece explicando que você está visualizando a versão da policy que estava ativa durante o período especificado e que desde então foi editada ou excluída.

Editar uma política ILM

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

Para editar uma política:

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



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

Clonar uma política ILM

Para clonar uma política ILM:

1. Selecione **ILM > Políticas**.
2. Selecione a caixa de seleção da política que você deseja clonar e, em seguida, selecione **Clonar**.
3. Crie uma nova política a partir da política que você clonou, seguindo as instruções em "[Criar políticas de ILM](#)".



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

Remover uma política ILM

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

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

Veja os detalhes da regra 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:

The screenshot shows the 'Rule detail' page for a rule named '2 copies 2 data centers'. At the top, there are three buttons: 'Clone', 'Edit', and 'Remove'. Below these are two tabs: 'Rule detail' (selected) and 'Used in policies'. The 'Rule detail' tab is divided into two sections: 'Time period and placements' and 'Retention diagram'. The 'Time period and placements' section has two sub-tabs: 'Retention diagram' (selected) and 'Placement instructions'. Under 'Retention diagram', there are two buttons: 'Time period' (selected) and 'Storage pool'. To the right of these buttons is a legend: a blue dot for 'Replicated copy' and a grey dot for 'Erasure-coded (EC) copy'. Below the legend is a 'Rule analysis' section with a bullet point: 'Objects processed by this rule will not be deleted by ILM.' The 'Retention diagram' section shows a timeline starting from 'Day 0' and going 'forever'. It displays two retention periods: '2 replicated copies - Data Center 1' (blue bar) and 'EC 2+1 - Data Center 1' (grey bar). The 'Duration' is indicated as 'Forever'.

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 estiver sendo usada em alguma política.

Clonar uma regra ILM

Você pode clonar uma regra existente se quiser criar uma nova regra que utilize algumas das configurações da regra existente. Se precisar editar uma regra que está sendo usada em alguma política, você clona a regra e faz as alterações no clone. Depois de fazer as 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 ILM se ela foi criada usando StorageGRID versão 10.2 ou anterior.

Passos

1. Selecione **ILM > Regras**.
2. Selecione a caixa de seleção da regra que você deseja clonar e, em seguida, 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 os passos para [editar uma regra ILM](#) e "[usando filtros avançados em regras ILM](#)".

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

Editar uma regra ILM

Você pode precisar editar uma regra ILM para alterar um filtro ou uma instrução de posicionamento.

Não é possível editar uma regra se ela estiver sendo usada em alguma política ILM. Em vez disso, você pode [clonar a regra](#) e fazer as alterações necessárias na cópia clonada.



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

Passos

1. Selecione **ILM > Regras**.
2. Confirme que a regra que você deseja editar não está sendo usada em nenhuma política 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 ILM. Se necessário, siga as etapas para "[criando uma regra ILM](#)" e "[usando filtros avançados em regras ILM](#)".

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

Remover uma regra ILM

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

Passos

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

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

1. Selecione a política inativa.
2. Remova a regra ILM da política ou [remover a policy](#).
3. Vá para os passos para remover uma regra ILM que não está sendo usada no momento.

Para remover uma regra ILM que não está sendo usada atualmente:

1. Selecione **ILM > Regras**.
2. Confirme que a regra que você deseja remover não está sendo 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 ao mesmo tempo.
4. Selecione **Sim** para confirmar que você deseja remover a regra ILM.

Visualizar métricas de ILM

Você pode visualizar métricas do 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 uma alta taxa de avaliação podem indicar que o sistema não está conseguindo acompanhar a taxa de ingestão, que a carga dos aplicativos cliente está excessiva ou que existe alguma condição anormal.

Passos

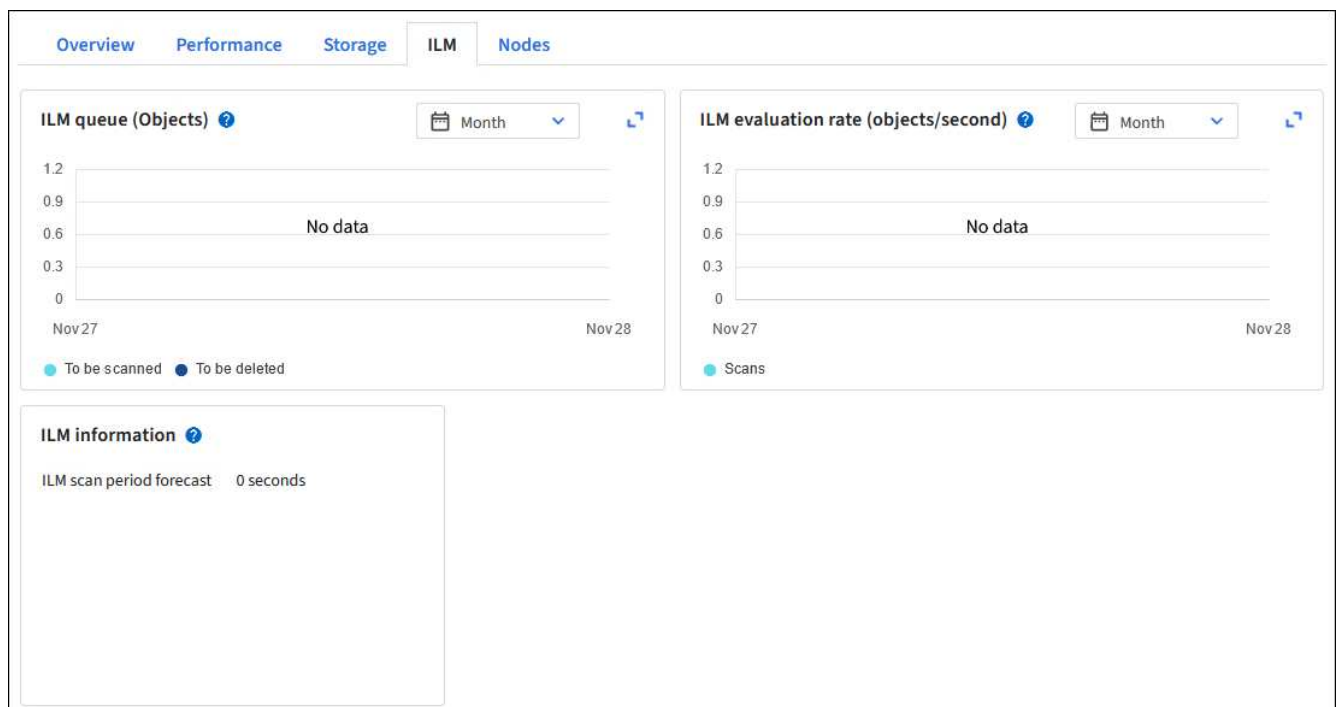
1. Selecione **Dashboard > ILM**.



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

2. Monitore as métricas na guia ILM.

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



Use o Bloqueio de Objeto S3

Como o S3 Object Lock protege objetos no StorageGRID

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

O que é o bloqueio de objeto S3?

O recurso StorageGRID S3 Object Lock é uma solução de proteção de objetos equivalente ao S3 Object Lock do Amazon Simple Storage Service (Amazon S3).

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

Um bucket sem S3 Object Lock só pode conter objetos sem configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

Um bucket com S3 Object Lock pode conter objetos com e sem configurações de retenção especificadas por aplicativos cliente S3. Alguns objetos ingeridos terão configurações de retenção.

Um bucket com S3 Object Lock 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, pois a configuração de retenção não foi definida no nível do objeto.

Na prática, todos os objetos recém-ingерidos têm configurações de retenção quando a retenção padrão está configurada. Os objetos existentes sem configurações de retenção 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 retain-until-date seja atingida.
 - A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.
 - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- Em 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 de objeto antes que a data de retenção seja atingida.
 - Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto.

Configurações de retenção para versões de objetos

Se um bucket for criado com o S3 Object Lock ativado, os usuários podem usar o aplicativo cliente S3 para, opcionalmente, especificar as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção:** conformidade ou governança.
- **Data de retenção:** Se a data de retenção de uma versão de objeto for futura, o objeto pode ser recuperado, mas não pode ser excluído.
- **Guarda legal:** Aplicar uma guarda legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar aplicar uma guarda legal a um objeto relacionado a uma investigação ou disputa legal. Uma guarda legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida. As guardas legais são independentes da data de retenção.



Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu modo de retenção.

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

Configuração padrão de retenção para buckets

Se um bucket for criado com o S3 Object Lock ativado, você pode, opcionalmente, especificar as seguintes configurações padrão para o bucket:

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

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

Veja ["Crie um bucket S3"](#) e ["Atualizar retenção padrão do S3 Object Lock"](#).

Comparando o S3 Object Lock com a Compliance legada

O recurso S3 Object Lock substitui o recurso Compliance 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 Compliance do StorageGRID, agora denominado "legacy Compliance".



A configuração de Compliance global está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração S3 Object Lock é habilitada automaticamente. Você pode continuar usando StorageGRID para gerenciar as configurações dos buckets compatíveis existentes; no entanto, você não pode criar novos buckets compatíveis. Para detalhes, veja ["NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"](#).

Se você utilizou o recurso de Compliance legado em uma versão anterior do StorageGRID, consulte a tabela a seguir para saber como ele se compara ao recurso S3 Object Lock no StorageGRID.

	Bloqueio de objeto S3	Conformidade (legado)
Como esse recurso é habilitado globalmente?	No Grid Manager, selecione Configuração > Sistema > S3 Object Lock .	Não é mais suportada.

	Bloqueio de objeto S3	Conformidade (legado)
Como o recurso é habilitado para um bucket?	Os usuários devem habilitar o S3 Object Lock ao criar um novo bucket usando o Tenant Manager, a Tenant Management API ou a API REST.	Não é mais suportada.
O versionamento de buckets é suportado?	Sim. O versionamento de buckets é necessário e é ativado automaticamente quando o S3 Object Lock está habilitado para o bucket.	Não
Como o período de retenção de objetos é definido?	Os usuários podem definir uma data limite de retenção para cada versão de 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, a data de retenção para uma versão de objeto pode ser aumentada, mas nunca diminuída. • 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 guarda legal é controlada?	Os usuários podem aplicar guarda legal ou remover guarda legal para qualquer versão de objeto no bucket.	Uma guarda legal é aplicada ao bucket e afeta todos os objetos no bucket.
Quando os objetos podem ser excluídos?	• No modo de conformidade, uma versão de objeto pode ser excluída após o retain-until-date ser atingido, desde que o objeto não esteja sob guarda legal. • No modo de governança, usuários com permissões especiais podem excluir um objeto antes que sua data de retenção seja atingida, desde que o objeto não esteja sob guarda legal.	Um objeto pode ser excluído após o período de retenção expirar, desde que o bucket não esteja sob guarda legal. Os objetos podem ser excluídos automaticamente ou manualmente.

	Bloqueio de objeto S3	Conformidade (legado)
A configuração de ciclo de vida do bucket é compatível?	Sim	Não

Fluxo de trabalho do S3 Object Lock no StorageGRID

Como administrador de grid, você deve coordenar-se de perto com os usuários locatários para garantir que os objetos sejam protegidos de uma forma que atenda aos requisitos de retenção deles.



A aplicação das configurações de locatário em toda a grid 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 grid e usuários locatários contêm as tarefas de alto nível para usar o recurso S3 Object Lock.

Administrador de grid

- Ative a configuração global de bloqueio de objetos S3 para todo o sistema StorageGRID.
- Garanta que as políticas de gerenciamento do ciclo de vida das informações (ILM) estejam em conformidade; ou seja, que atendam aos ["Requisitos de buckets com S3 Object Lock ativado"](#).
- Se necessário, permita que um locatário use o modo de Compliance como modo de retenção. Caso contrário, somente o modo de Governance é permitido.
- Se necessário, defina um período máximo de retenção para um tenant.

Usuário locatário

- Analise as considerações para buckets e objetos com S3 Object Lock.
- Se necessário, entre em contato com o administrador da grid para ativar a configuração global de S3 Object Lock e definir as permissões.
- Crie buckets com o S3 Object Lock ativado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
 - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da grid.
 - Período de retenção padrão: deve ser menor ou igual ao período de retenção máximo 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 grid.
 - Data de retenção: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador do grid.

Requisitos do S3 Object Lock no StorageGRID

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

Requisitos para usar a configuração global de S3 Object Lock

- Você precisa habilitar a configuração global de S3 Object Lock usando o Grid Manager ou a Grid Management API antes que qualquer tenant S3 possa criar um bucket com S3 Object Lock habilitado.
- Habilitar a configuração global de S3 Object Lock permite que todas as contas de locatário do S3 criem buckets com S3 Object Lock ativado.
- Depois de ativar a configuração global de S3 Object Lock, você não poderá desativar a configuração.
- Você não pode habilitar o S3 Object Lock global a menos que a regra padrão em todas as políticas ILM ativas seja *compliant* (ou seja, a regra padrão deve estar em conformidade com os requisitos dos buckets com S3 Object Lock habilitado).
- Quando a configuração global de S3 Object Lock está ativada, você não pode criar uma nova política ILM nem ativar uma política ILM existente, a menos que a regra padrão na política seja compatível. Depois que a configuração global de S3 Object Lock for ativada, as páginas de regras ILM e políticas ILM indicam quais regras ILM são compatíveis.

Requisitos para regras ILM em conformidade

Se você deseja habilitar a configuração global de S3 Object Lock, você deve garantir que a regra padrão em todas as políticas ILM ativas esteja em conformidade. Uma regra em conformidade atende aos requisitos tanto dos buckets com S3 Object Lock habilitado quanto de quaisquer buckets existentes que tenham Compliance legada habilitada:

- É necessário criar pelo menos duas cópias replicadas do objeto ou uma cópia com código de apagamento.
- Essas cópias devem existir nos Storage Nodes durante toda a duração de cada linha nas instruções de posicionamento.
- Não é possível salvar cópias de objetos em um Cloud Storage Pool.
- Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando **Horário de ingestão** como tempo de referência.
- Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

Requisitos para políticas de ILM

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

- A regra padrão em uma política ILM ativa ou inativa deve estar em conformidade.
- As regras de não conformidade aplicam-se apenas a objetos em buckets que não têm o S3 Object Lock ativado ou que não têm o recurso de Compliance legado ativado.
- As regras de conformidade podem ser aplicadas a objetos em qualquer bucket; S3 Object Lock ou Compliance legada não precisam estar habilitados para o bucket.

"Exemplo de uma política ILM compatível para S3 Object Lock"

Requisitos para buckets com S3 Object Lock ativado

- Se a configuração global de S3 Object Lock estiver habilitada para o sistema StorageGRID, você pode usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com S3 Object Lock habilitado.

- Se você planeja usar o S3 Object Lock, precisa habilitar o S3 Object Lock ao criar o bucket. Você não pode habilitar o S3 Object Lock para um bucket existente.
- Quando o S3 Object Lock está habilitado para um bucket, o StorageGRID habilita automaticamente o versionamento para esse bucket. Você não pode desabilitar o S3 Object Lock nem suspender o versionamento para o 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 uma data de retenção para cada versão do objeto no momento do upload.
- A configuração do ciclo de vida do bucket é compatível com buckets que possuem o S3 Object Lock ativado.
- CloudMirror A replicação não é suportada para buckets com S3 Object Lock ativado.

Requisitos para objetos em buckets com S3 Object Lock ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou pode especificar configurações de retenção para cada versão de objeto. As configurações de retenção em nível de objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST.
- As configurações de retenção se aplicam a versões individuais de objetos. Uma versão de objeto pode ter tanto uma configuração de data de retenção quanto de guarda legal, uma delas, mas não a outra, ou nenhuma das duas. Especificar uma data de retenção ou uma configuração de guarda 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 S3 Object Lock ativado

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

1. Ingestão de objeto

Quando uma versão de objeto é adicionada a um bucket com o S3 Object Lock ativado, as configurações de retenção são aplicadas da seguinte forma:

- Se as configurações de retenção forem especificadas para o objeto, as configurações em nível de objeto serão aplicadas. Quaisquer configurações padrão de bucket serão ignoradas.
- Se nenhuma configuração de retenção for especificada para o objeto, as configurações padrão do bucket serão aplicadas, se existirem.
- Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não estará protegido pelo S3 Object Lock.

Se as configurações de retenção forem aplicadas, tanto o objeto quanto quaisquer metadados definidos pelo usuário S3 estarão 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 objeto, assim como os locais de armazenamento, são determinados pelas regras de conformidade nas políticas ILM ativas. Se um objeto protegido pode ser excluído antes de atingir sua data de retenção depende do seu modo de retenção.

- Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu

modo de retenção.

Informações relacionadas

- ["Crie um bucket S3"](#)
- ["Atualizar retenção padrão do S3 Object Lock"](#)
- ["Use a API REST S3 para configurar o S3 Object Lock"](#)
- ["Exemplo 7: política ILM compatível para S3 Object Lock"](#)

Ativar o S3 Object Lock globalmente no StorageGRID

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

Antes de começar

- Você tem o ["Permissão de acesso root"](#).
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você analisou o fluxo de trabalho de S3 Object Lock e compreende as considerações.
- Você confirmou que a regra padrão na política ILM ativa está em conformidade. Veja ["Criar uma regra ILM padrão"](#) para detalhes.

Sobre esta tarefa

Um administrador de grid deve habilitar a configuração global de Bloqueio de Objetos S3 para permitir que os usuários do tenant criem novos buckets com o Bloqueio de Objetos S3 habilitado. Depois de habilitada, essa configuração não pode ser desabilitada.

Revise as configurações de conformidade dos locatários existentes após ativar a configuração global de S3 Object Lock. Ao ativar essa configuração, as configurações de S3 Object Lock por locatário dependem da versão do StorageGRID vigente no momento em que o locatário foi criado.



A configuração de Compliance global está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração S3 Object Lock é habilitada automaticamente. Você pode continuar usando StorageGRID para gerenciar as configurações dos buckets compatíveis existentes; no entanto, você não pode criar novos buckets compatíveis. Para detalhes, veja ["NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"](#).

Passos

1. Selecione **Configuração > Sistema > S3 Object Lock**.

A página Configurações de bloqueio de objetos S3 é exibida.

2. Selecione **Ativar S3 Object Lock**.
3. Selecione **Aplicar**.

Uma caixa de diálogo de confirmação é exibida e lembra você de que não é possível desativar o S3 Object Lock depois que ele é ativado.

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

Ao selecionar **OK**:

- Se a regra padrão na política ILM ativa estiver em conformidade, o S3 Object Lock agora está ativado para toda a grid e não pode ser desativado.
- Se a regra padrão não for compatível, um erro será exibido. Você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política, simule-a e ative-a. Consulte "[Criar política de ILM](#)" para obter instruções.

Resolva erros de consistência ao atualizar S3 Object Lock ou configurações de Compliance legadas no StorageGRID

Caso um site de data center ou vários Storage Nodes em um site fiquem indisponíveis, você poderá precisar ajudar os usuários do tenant do S3 a aplicar alterações no S3 Object Lock ou na configuração de Compliance legada.

Usuários locatários que possuem buckets com S3 Object Lock (ou Compliance legada) ativado podem alterar determinadas configurações. Por exemplo, um usuário locatário que utiliza S3 Object Lock pode precisar colocar uma versão de objeto sob guarda legal.

Quando um usuário locatário atualiza as configurações de um bucket S3 ou a versão de um objeto, StorageGRID tenta atualizar imediatamente os metadados do bucket ou do objeto em toda a grid. Se o sistema não conseguir atualizar os metadados porque um site do data center ou vários Storage Nodes estão indisponíveis, ele retorna 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 estes passos:

1. Tente disponibilizar todos os Storage Nodes ou sites novamente o mais rápido possível.
2. Caso não consiga disponibilizar nós de armazenamento suficientes em cada local, entre em contato com o suporte técnico, que pode ajudar você a recuperar os nós e garantir que as alterações sejam aplicadas de forma consistente em toda a grid.
3. Após a resolução do problema subjacente, lembre o usuário locatário de tentar novamente as alterações de configuração.

Informações relacionadas

- "[Use uma conta de tenant](#)"
- "[Utilize a API REST S3](#)"
- "[Recuperar e manter](#)"

Exemplos de regras e políticas de ILM

Regras e políticas do ILM para proteção básica de objetos e retenção no StorageGRID

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



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

Regra 1 do ILM para o exemplo 1: copiar dados de objeto para dois sites

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

Definição de regra	Valor de exemplo
Pools de storage em um único site	Dois pools de storage, cada um contendo sites diferentes, chamados Site 1 e Site 2.
Nome da regra	Duas cópias dois sites
Tempo de referência	Tempo de ingestão
Atribuições	Do dia 0 até a perpetuidade, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

A seção de 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 não serão excluídos pelo ILM.

Reference time ?

Ingest time

Time period and placements

Sort by start date

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

Time period 1
From Day 0
store forever

Store objects by replicating 1 copies at Site 1

and store objects by replicating 1 copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

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

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

Regra 2 do ILM para o exemplo 1: Perfil de codificação de apagamento com correspondência de bucket

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

Definição de regra	Valor de exemplo
Pool de storage com vários sites	- Um único pool de storage em três sites (Sites 1, 2, 3) - Use o esquema de codificação de apagamento 6+3
Nome da regra	Bucket S3 finance-records
Tempo de referência	Tempo de ingestão
Atribuições	Para os objetos no bucket S3 chamado finance-records, crie uma cópia codificada de apagamento no pool especificado pelo perfil de codificação de apagamento. Mantenha essa cópia para sempre.

Time period and placements

Sort by start date

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

Time period 1

From Day 0

store

forever

Store objects by

erasure coding

using

6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

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

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration

Forever

Política ILM para o exemplo 1

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

Uma política ILM típica para uma grid multi-site pode incluir regras ILM como as seguintes:

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

Proposed policy name

Object Storage Policy

Reason for change

example 1

Manage rules

1. Select the rules you want to add to the policy.

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

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informações relacionadas

- ["Use políticas ILM"](#)
- ["Criar políticas de ILM"](#)

Regras e política de ILM para filtragem de tamanho de objetos EC no StorageGRID

Você pode usar as seguintes regras e políticas de exemplo como ponto de partida para definir uma política ILM que filtre por tamanho de objeto para atender aos requisitos recomendados de codificação de apagamento.



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

Regra 1 do ILM para o exemplo 2: use EC para objetos maiores que 1 MB

Este exemplo de regra ILM aplica codificação de apagamento a objetos com mais de 1 MB.



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

Definição de regra	Valor de exemplo
Nome da regra	Apenas objetos de EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Atribuições	Crie uma cópia 2+1 com codificação de apagamento usando três sites

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

Object size ▼

greater than ▼

1 ⬆ ⬇ ⬆

MB ▼ ×

Regra 2 do ILM para o exemplo 2: duas cópias replicadas

Esta regra de exemplo do ILM cria duas cópias replicadas e não filtra por tamanho do objeto. Esta regra é a regra padrão da política. Como a primeira regra filtra todos os objetos maiores que 1 MB, esta regra se aplica somente 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
Atribuições	Do dia 0 até a perpetuidade, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

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

Esta política ILM de exemplo inclui duas regras ILM:

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

Regras e política de ILM para proteger arquivos de imagem no StorageGRID

Você pode usar as seguintes regras e políticas de exemplo para garantir que imagens maiores que 1 MB sejam codificadas de apagamento e que duas cópias sejam feitas de imagens menores.



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

Regra 1 do ILM para o exemplo 3: use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para aplicar codificação de apagamento a todos os arquivos de imagem maiores que 1 MB.



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

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 superior a 1 MB
Filtros avançados para chave	• Termina com .jpg • Termina com .png

Definição de regra	Valor de exemplo
Atribuições	Crie uma cópia 2+1 com codificação de apagamento usando três sites

The screenshot shows the configuration for two filter groups in an ILM policy. Each group is defined by a set of conditions that must be met for an object to be evaluated by the rule.

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

- Object size: greater than 1 MB
- and Key: ends with .jpg

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

- Object size: greater than 1 MB
- and Key: ends with .png

Como essa regra está configurada como a primeira regra na política, a instrução de colocação de codificação de apagamento se aplica somente a arquivos .jpg e .png com mais de 1 MB.

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

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

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
Atribuições	Crie 2 cópias replicadas em dois pools de storage

Política ILM para o exemplo 3: melhor proteção para arquivos de imagem

Esta política ILM de exemplo inclui três regras:

- A primeira regra codifica por apagamento 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 menores).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam imagens).

Rule order	Rule name	Filters
1	↕ EC image files > 1 MB	Object size is greater than 1 MB
2	↕ 2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Regras e políticas de ILM para versões não atuais de objetos S3 no StorageGRID

Se você tiver um bucket S3 com versionamento ativado, poderá gerenciar as versões desatualizadas dos objetos incluindo regras em sua política ILM que usem o "Tempo desatualizado" como tempo de referência.



Se você especificar um tempo de retenção limitado para os objetos, esses objetos serão excluídos permanentemente após o término desse período. Certifique-se de compreender 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 alocação diferentes para versões não atuais do objeto.



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



Para realizar a simulação da política ILM em uma versão não atual de um objeto, você precisa saber o UUID ou CBID da versão do objeto. Para encontrar o UUID e o CBID, use ["pesquisa de metadados de objetos"](#) enquanto o objeto ainda estiver atual.

Informações relacionadas

["Como os objetos são excluídos"](#)

Regra 1 do ILM para o exemplo 4: Salve três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três sites por 10 anos.

Essa regra se aplica a todos os objetos, independentemente de serem ou não versionados.

Definição de regra	Valor de exemplo
Pools de storage	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

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no Site 1, uma no Site 2 e uma no Site 3. Ao final de 10 anos, exclua todas as cópias do objeto.

Regra 2 do ILM para o exemplo 4: salve duas cópias de versões não atuais por 2 anos

Esta regra ILM de exemplo 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 use "Tempo não atual" como tempo de referência, selecione **Sim** na pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" na Etapa 1 (Inserir detalhes) do assistente Criar uma regra ILM. Ao selecionar **Sim**, *Tempo não atual* é selecionado automaticamente como tempo de referência e você não pode selecionar um tempo de referência diferente.

1 Enter details

2 Define placements

3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No
☒ Yes

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 um data center diferente, Site 1 e Site 2.
Nome da regra	Versões não atuais: duas cópias dois anos
Tempo de referência	Tempo não atual Selecionada automaticamente quando você seleciona Sim para a pergunta, "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" no assistente Criar uma regra ILM.
Atribuições	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 exemplo 4: objetos versionados do S3

Se você deseja gerenciar versões 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 ILM antes das regras que se aplicam à versão atual do objeto.

Uma política ILM para objetos versionados do S3 pode incluir regras ILM como as seguintes:

- Mantenha quaisquer versões 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 não atuais do objeto nunca serão correspondidas pela regra de "Tempo não atual".

- No momento da 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 forma:

- Qualquer versão de objeto não atual será correspondida pela primeira regra. Se uma versão de objeto não atual tiver mais de 2 anos, ela é excluída permanentemente pelo ILM (todas as cópias da versão não atual removidas do grid).
- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto estiver 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 avaliação do ILM, essa versão não atual será correspondida pela primeira regra. Como resultado, a cópia no Site 3 é excluída e as duas cópias nos Sites 1 e 2 são armazenadas por mais 2 anos.

Regras e política de ILM para comportamento de ingestão estrito no StorageGRID

Você pode usar um filtro de local e o comportamento de ingestão estrito em uma regra para impedir que os objetos sejam salvos em um local específico do data center.

Neste exemplo, um locatário com sede em Paris não deseja 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 regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que 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 para o exemplo 5: Ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra ILM usa o comportamento de ingestão estrito para garantir que os objetos salvos por um locatário com sede em Paris em buckets S3 com a região definida como eu-west-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra aplica-se a objetos que pertencem ao locatário Paris e que têm a região do bucket S3 definida como eu-west-3 (Paris).

Definição de regra	Valor de exemplo
Conta de tenant	Tenant Paris
Filtro avançado	A restrição de local é igual a eu-west-3
Pools de storage	Local 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Atribuições	No dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Rigoroso. Sempre utilize os posicionamentos desta regra na ingestão. A ingestão falhará se não for possível armazenar duas cópias do objeto no data center de Paris.

Strict ingest to guarantee Paris data center

Compliant: Yes
Used in active policy: No
Used in proposed policy: No

Ingest behavior: Strict
Reference time: Ingest time

Clone Edit Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool ● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

Regra 2 do ILM para o exemplo 5: ingestão balanceada para outros objetos

Esta regra de ILM de exemplo usa o comportamento de ingestão balanceada para fornecer eficiência ideal de ILM para quaisquer objetos que não correspondam à primeira regra. Duas cópias de todos os objetos correspondentes a esta regra serão armazenadas: uma no data center dos EUA e uma no data center de Paris. Se a regra não puder ser atendida imediatamente, cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra aplica-se a objetos que pertencem a qualquer tenant e a qualquer região.

Definição de regra	Valor de exemplo
Conta de tenant	Ignorar
Filtro avançado	<i>Não especificado</i>
Pools de storage	Local 1 (Paris) e Local 2 (US)
Nome da regra	2 Cópias 2 Data Centers
Tempo de referência	Tempo de ingestão

Definição de regra	Valor de exemplo
Atribuições	No dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Os objetos que correspondem a esta regra são colocados de acordo com as instruções de posicionamento da regra, se possível. Caso contrário, cópias provisórias são feitas em qualquer local disponível.

Política ILM para o exemplo 5: combinando comportamentos de ingestão

A política ILM de exemplo inclui duas regras com comportamentos de ingestão diferentes.

Uma política ILM que utiliza dois comportamentos de ingestão diferentes pode incluir regras ILM como as seguintes:

- Armazene os objetos pertencentes ao locatário de Paris e que tenham a região do bucket S3 definida como eu-west-3 (Paris) somente no data center de Paris. Falhe a 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) tanto no data center dos EUA quanto no data center de Paris. Faça cópias provisórias em qualquer local disponível caso a instrução de posicionamento não possa ser atendida.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Quaisquer objetos pertencentes ao locatário de Paris e que tenham 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 falha.
- Todos os outros objetos são correspondidos pela segunda regra, incluindo objetos pertencentes 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 data center. No entanto, como a segunda regra usa Balanced ingest, se um data center estiver indisponível, duas cópias provisórias são salvas em qualquer local disponível.

Como a alteração de uma política ILM afeta o desempenho do StorageGRID

Se precisar alterar sua proteção de dados ou adicionar novos sites, você pode criar e ativar uma nova política ILM.

Antes de alterar uma política, você deve entender como as mudanças 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 ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro **"criar uma política"**. Em seguida, você deve **"simular"** e depois **"ativar"** a nova política.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que 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 ILM, o desempenho do seu sistema StorageGRID pode ser afetado temporariamente, especialmente se as instruções de posicionamento na nova política exigirem que muitos objetos existentes sejam movidos para novos locais.

Ao ativar uma nova política ILM, StorageGRID a utiliza para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política ILM, revise quaisquer alterações no posicionamento de objetos replicados e objetos com codificação de apagamento 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 ILM não afete a alocação de objetos replicados e codificados para apagamento existentes, você pode "[Crie uma regra ILM com um filtro de tempo de ingestão](#)". Por exemplo, **Ingest time is on or after <date and time>**, para que a nova regra se aplique somente a objetos ingeridos na data e hora especificadas ou posteriormente.

Os tipos de alterações de política ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

- Aplicando um perfil de codificação de apagamento diferente a objetos já codificados por apagamento.



StorageGRID considera cada perfil de codificação de apagamento como único e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos com codificação de apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos para ou de um Cloud Storage Pool ou para ou de um local remoto.

Política ILM ativa, por exemplo 6: proteção de dados em dois locais

Neste exemplo, a política ILM ativa foi inicialmente projetada para um sistema StorageGRID de dois locais e utiliza duas regras ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

Nessa política de ILM, os objetos pertencentes ao Tenant A são protegidos por codificação de apagamento 2+1 em um único site, enquanto os objetos pertencentes a todos os outros tenants são protegidos em dois sites usando replicação de 2 cópias.

Regra 1: codificação de apagamento em um único site para o Tenant A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de apagamento de um único local para o tenant A
Conta de tenant	Locatário A
Pool de storage	Local 1
Atribuições	codificação de apagamento 2+1 no Site 1 do dia 0 até sempre

Regra 2: replicação em dois locais para outros inquilinos

Definição de regra	Valor de exemplo
Nome da regra	Replicação em dois locais para outros tenants
Conta de tenant	Ignorar
Pools de armazenamento	Site 1 e Site 2
Atribuições	Duas cópias replicadas desde o dia 0 até a eternidade: uma cópia no Site 1 e uma cópia no Site 2.

Política ILM para exemplo 6: proteção de dados em três locais

Neste exemplo, a política ILM está sendo substituída por uma nova política para um sistema StorageGRID de três locais.

Após realizar uma expansão para adicionar o novo site, o administrador da grade criou dois novos pools de storage: um pool de storage para o Site 3 e um pool de storage contendo todos os três sites (não é o mesmo que o pool de storage padrão All Storage Nodes). Em seguida, o administrador criou duas novas regras ILM e uma nova política ILM, projetada para proteger os dados em todos os três sites.

Quando essa nova política ILM for ativada, os objetos pertencentes ao Tenant A serão protegidos por codificação de apagamento 2+1 em três sites, enquanto os objetos pertencentes a outros tenants (e objetos menores pertencentes ao Tenant A) serão protegidos em três sites usando replicação de 3 cópias.

Regra 1: codificação de apagamento em três sites para o Tenant A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de apagamento de três locais para o tenant A

Definição de regra	Valor de exemplo
Conta de tenant	Locatário A
Pool de storage	Todos os 3 sites (inclui o Site 1, o Site 2 e o Site 3)
Atribuições	codificação de apagamento 2+1 em todos os 3 sites do dia 0 para sempre

Regra 2: replicação em três locais para outros tenants

Definição de regra	Valor de exemplo
Nome da regra	Replicação em três locais para outros tenants
Conta de tenant	Ignorar
Pools de armazenamento	Site 1, Site 2 e Site 3
Atribuições	Três cópias replicadas desde o dia 0 até a eternidade: uma cópia no Site 1, uma cópia no Site 2 e uma cópia no Site 3.

Ativando a política ILM para o exemplo 6

Ao ativar uma nova política ILM, os 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 de dados irrecuperável. Analise e simule cuidadosamente a política antes de ativá-la para confirmar que ela funcionará conforme o esperado.



Ao ativar uma nova política ILM, StorageGRID a utiliza para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política ILM, revise quaisquer alterações no posicionamento de objetos replicados e objetos com codificação de apagamento 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 Tenant A são protegidos usando codificação de apagamento 2+1 no Site 1. Na nova política ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2+1 nos Sites 1, 2 e 3.

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

- Novos objetos recebidos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Em seguida, cada um dos três fragmentos é armazenado em um site diferente.

- Os objetos existentes pertencentes ao Tenant A são reavaliados durante o processo de varredura ILM em andamento. Como as instruções de posicionamento do ILM utilizam um novo perfil de codificação de apagamento, fragmentos de codificação de apagamento totalmente novos são criados e distribuídos para os três sites.



Os fragmentos 2+1 existentes no Site 1 não são reutilizados. StorageGRID considera cada perfil de codificação de apagamento como único e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política ILM atualmente ativa para este exemplo, os objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de storage nos Sites 1 e 2. Na nova política ILM, os objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de storage nos Sites 1, 2 e 3.

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

- Quando qualquer locatário que não seja o Tenant A ingere um novo objeto, StorageGRID cria três cópias e salva uma cópia em cada site.
- Os objetos existentes pertencentes a esses outros locatários são reavaliados durante o processo contínuo de verificação 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, StorageGRID precisa criar apenas uma nova cópia do objeto para o Site 3.

Impacto no desempenho de ativar esta política

Quando a política ILM deste exemplo for ativada, o desempenho geral deste StorageGRID será afetado temporariamente. Serão necessários níveis de recursos de grid superiores ao normal para criar novos fragmentos com codificação de apagamento para os objetos existentes do Tenant A e novas cópias replicadas no Site 3 para os objetos existentes de outros tenants.

Como resultado da alteração na política ILM, as solicitações de leitura e gravação do cliente podem apresentar latências temporariamente maiores que o normal. As latências retornarão aos níveis normais após a implementação completa das instruções de posicionamento em todo o grid.

Para evitar problemas de recursos ao ativar uma nova política ILM, você pode usar o filtro avançado Ingest time em qualquer regra que possa alterar a localização de um grande número de objetos existentes. Defina Ingest time para um valor maior ou igual ao horário aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.



Contate o suporte técnico se você precisar diminuir ou aumentar a velocidade com que os objetos são processados após uma alteração na política do ILM.

Política ILM compatível para S3 Object Lock no StorageGRID

Você pode usar o bucket S3, as regras ILM e a política ILM deste exemplo como ponto de partida ao definir uma política ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o S3 Object Lock ativado.



Se você utilizou o recurso de Compliance legado em versões anteriores do StorageGRID, também pode usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de Compliance legado ativado.



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

Informações relacionadas

- ["Gerencie objetos com S3 Object Lock"](#)
- ["Crie uma política ILM"](#)

Bucket e objetos para exemplo de S3 Object Lock

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Tenant Manager para criar um bucket com S3 Object Lock ativado para armazenar registros bancários críticos.

Definição de bucket	Valor de exemplo
Nome da conta do locatário	Bank of ABC
Nome do bucket	registros bancários
Região do bucket	us-east-1 (padrão)

Cada objeto e versão de objeto adicionados ao bucket bank-records usarão os seguintes valores para `retain-until-date` e `legal hold` configurações.

Configuração para cada objeto	Valor de exemplo
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 de dezembro de 2030) Cada versão do objeto possui sua própria <code>retain-until-date</code> configuração. Essa configuração pode ser aumentada, mas não diminuída.
<code>legal hold</code>	"DESLIGADO" (não está em vigor) Uma guarda legal pode ser aplicada ou removida de qualquer versão de um objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob guarda legal, ele não poderá ser excluído, mesmo que o <code>retain-until-date</code> tenha sido atingido.

Exemplo da regra 1 do ILM para S3 Object Lock: perfil de codificação de apagamento com correspondência de bucket

Este exemplo de regra de ILM aplica-se apenas à conta de tenant S3 chamada Bank of ABC. Ela corresponde a qualquer objeto no `bank-records` bucket e, em seguida, utiliza codificação de apagamento para armazenar o objeto em Storage Nodes em três data center, usando um perfil de codificação de apagamento

6+3. Esta regra atende aos requisitos de buckets com S3 Object Lock ativado: uma cópia é mantida em Storage Nodes do dia 0 para sempre, usando o horário 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 - Bank of ABC
Conta de tenant	Bank of ABC
Nome do bucket	bank-records
Filtro avançado	Tamanho do objeto (MB) maior que 1 Nota: Este filtro garante que codificação de apagamento não seja usada para objetos de 1 MB ou menores.

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	Desde o dia 0, armazene para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada por apagamento em Storage Nodes em três sites de data center • Utiliza o esquema de codificação de apagamento 6+3

Regra ILM 2 para S3 Object Lock: regra não compatível

Este exemplo de regra ILM armazena inicialmente duas cópias replicadas de objetos em Storage Nodes. Após um ano, armazena uma cópia em um Cloud Storage Pool para sempre. Como essa regra usa um Cloud Storage Pool, ela não está em conformidade e não será aplicada aos objetos em buckets com S3 Object Lock ativado.

Definição de regra	Valor de exemplo
Nome da regra	Regra não conforme: usar o Cloud Storage Pool
Contas de locatários	Não especificado
Nome do bucket	Não especificado, mas só se aplicará a buckets que não tenham S3 Object Lock (ou o recurso legado Compliance) ativado.
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	• No dia 0, mantenha duas cópias replicadas nos Storage Nodes no Data Center 1 e no Data Center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um Cloud Storage Pool para sempre

Regra 3 do ILM para S3 Object Lock: regra padrão

Esta regra de exemplo do ILM copia dados de objetos para pools de storage em dois data centers. Esta regra em conformidade foi projetada para ser a regra padrão na política do ILM. Ela não inclui filtros, não usa o tempo de referência Noncurrent e atende aos requisitos de buckets com S3 Object Lock ativado: duas cópias do objeto são mantidas nos Storage Nodes do dia 0 para sempre, usando Ingest como tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra padrão de conformidade: Duas cópias dois data centers
Conta de tenant	Não especificado
Nome do bucket	Não especificado
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	Do dia 0 em diante, mantenha duas cópias replicadas: uma nos Storage Nodes no Data Center 1 e outra nos Storage Nodes no Data Center 2.

Exemplo de política ILM compatível para S3 Object Lock

Para criar uma política ILM que proteja efetivamente todos os objetos do seu sistema, incluindo aqueles em buckets com S3 Object Lock ativado, você deve selecionar regras ILM que atendam aos requisitos de armazenamento de todos os objetos. Em seguida, você deve simular e ativar a política.

Adicionar regras à política

Neste exemplo, a política ILM inclui três regras ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de apagamento para proteger objetos maiores que 1 MB em um bucket específico com S3 Object Lock ativado. Os objetos são armazenados em Storage Nodes do dia 0 para sempre.
2. Uma regra não conforme que cria duas cópias replicadas de objetos em Storage Nodes por um ano e, em seguida, move uma das cópias para um Cloud Storage Pool permanentemente. Essa regra não se aplica a buckets com S3 Object Lock ativado porque utiliza um Cloud Storage Pool.

3. A regra padrão de conformidade que cria duas cópias replicadas de objetos em Storage Nodes desde o primeiro dia até indefinidamente.

Simule a política

Depois de adicionar regras à sua política, escolher uma regra padrão compatível e organizar as demais regras, você deve simular a política testando objetos do bucket com S3 Object Lock ativado e de outros buckets. Por exemplo, ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- A primeira regra só corresponderá a objetos de teste que sejam maiores que 1 MB no bucket bank-records para o tenant Bank of ABC.
- A segunda regra corresponderá a todos os objetos em todos os buckets não compatíveis para todas as outras contas de tenant.
- A regra padrão corresponderá a estes objetos:
 - Objetos de 1 MB ou menores no bucket bank-records para o tenant Bank of ABC.
 - Objetos em qualquer outro bucket que tenha o S3 Object Lock ativado para todas as outras contas de locatário.

Ative a política

Quando você estiver completamente satisfeito de que a nova política protege os dados do objeto conforme o esperado, você pode ativá-la.

Como o ciclo de vida do bucket S3 e a política ILM interagem no StorageGRID

Dependendo da sua configuração de ciclo de vida, os objetos seguem as configurações de retenção do ciclo de vida do bucket S3 ou de uma política ILM.

Exemplo de ciclo de vida do bucket tendo prioridade sobre a política ILM

Política ILM

- Regra baseada em referência a um período anterior ao 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 bucket

```
"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 com o prefixo "docs/".
 - Após 100 dias, um marcador de exclusão é criado e "docs/text" se torna não atual.
 - Após 5 dias, num total de 105 dias desde a ingestão, "docs/text" é excluída.
 - Após 95 dias, totalizando 200 dias desde a ingest e 100 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.
- Um objeto chamado "video/movie" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.

- Após 50 dias, um marcador de exclusão é criado e "video/movie" se torna não atual.
- Após 20 dias, totalizando 70 dias desde a ingestão, "vídeo/filme" é excluído.
- Após 30 dias, totalizando 100 dias desde a ingest e 50 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.

Exemplo de ciclo de vida de bucket que implicitamente mantém para sempre

Política ILM

- Regra baseada em referência a um período anterior ao 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 bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker": true}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket com o prefixo "docs/".

A `Expiration`ação se aplica apenas 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 "video/movie" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.
 - Após 50 dias, um marcador de exclusão é criado e "video/movie" se torna não atual.
 - Após 20 dias, totalizando 70 dias desde a ingestão, "vídeo/filme" é excluído.
 - Após 30 dias, totalizando 100 dias desde a ingest 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 ILM

- Regra baseada em referência a um período anterior ao 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 para sempre

Ciclo de vida do bucket

```
"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 de ILM foi projetada para remover objetos manualmente e limpar versões não atuais após 20 dias. Consequentemente, a regra de ingestão manterá os marcadores de exclusão expirados para sempre.
 - O ciclo de vida do bucket duplica o comportamento da política ILM

"ExpiredObjectDeleteMarker": true, que remove marcadores de exclusão assim que expiram

- Um objeto é ingerido. A ausência de 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 se torna expirado.
 - Logo em seguida, o marcador de exclusão expirado é excluído.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.