Solução de problemas de objetos e storage

StorageGRID

NetApp
October 03, 2025

Índice

Solução de problemas de objetos e storage

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas de armazenamento e objeto.

Confirmar localizações de dados do objeto

Dependendo do problema, você pode querer confirmar onde os dados do objeto estão sendo armazenados. Por exemplo, você pode querer verificar se a política ILM está funcionando como esperado e os dados do objeto estão sendo armazenados onde se pretende.

O que você vai precisar

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

Passos

1. Selecione **ILM** > **Object Metadata Lookup**.
2. Digite o identificador do objeto no campo **Identificador**.

   Você pode inserir um UUID, CBID, S3 bucket/object-key ou Swift container/object-name.

3. Clique em **Procurar**.

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

   - Metadados do sistema, incluindo o ID do objeto (UUID), o nome do objeto, o nome do contentor, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
   - Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
   - Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
   - Para cópias de objetos replicadas, o local de storage atual de cada cópia.
   - Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.

- Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos de várias partes, uma lista de segmentos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os primeiros 100 segmentos são mostrados.
- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não são garantidos para persistir de liberação para liberação.

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

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Informações relacionadas

"Gerenciar objetos com ILM"

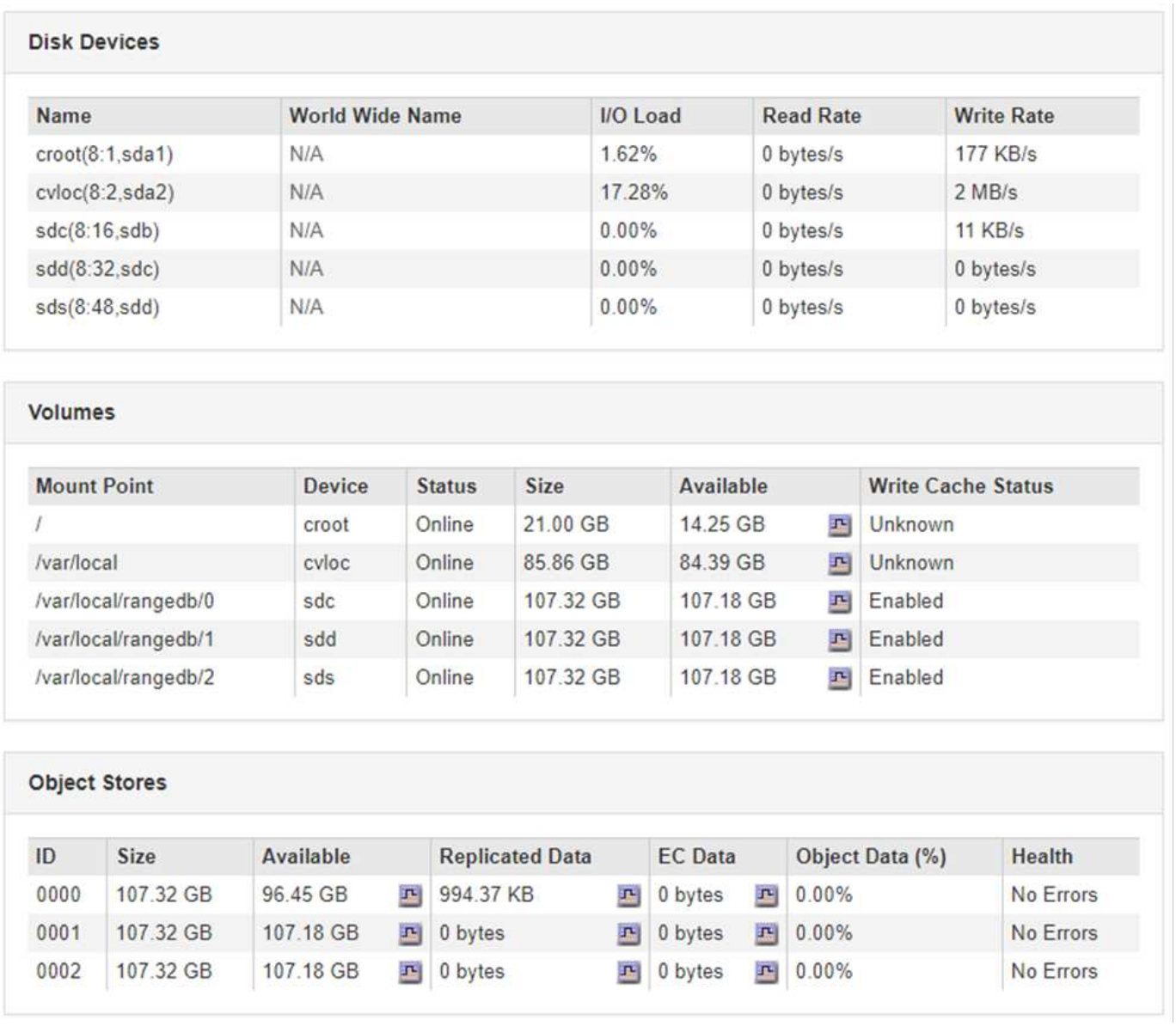
"Use S3"

"Use Swift"

Falhas no armazenamento de objetos (volume de storage)

O storage subjacente em um nó de storage é dividido em armazenamentos de objetos. Esses armazenamentos de objetos são partições físicas que atuam como pontos de montagem para o armazenamento do sistema StorageGRID. Os armazenamentos de objetos também são conhecidos como volumes de armazenamento.

Você pode exibir informações de armazenamento de objetos para cada nó de armazenamento. Os armazenamentos de objetos são mostrados na parte inferior da página **nós *Storage Node* Storage**.



Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

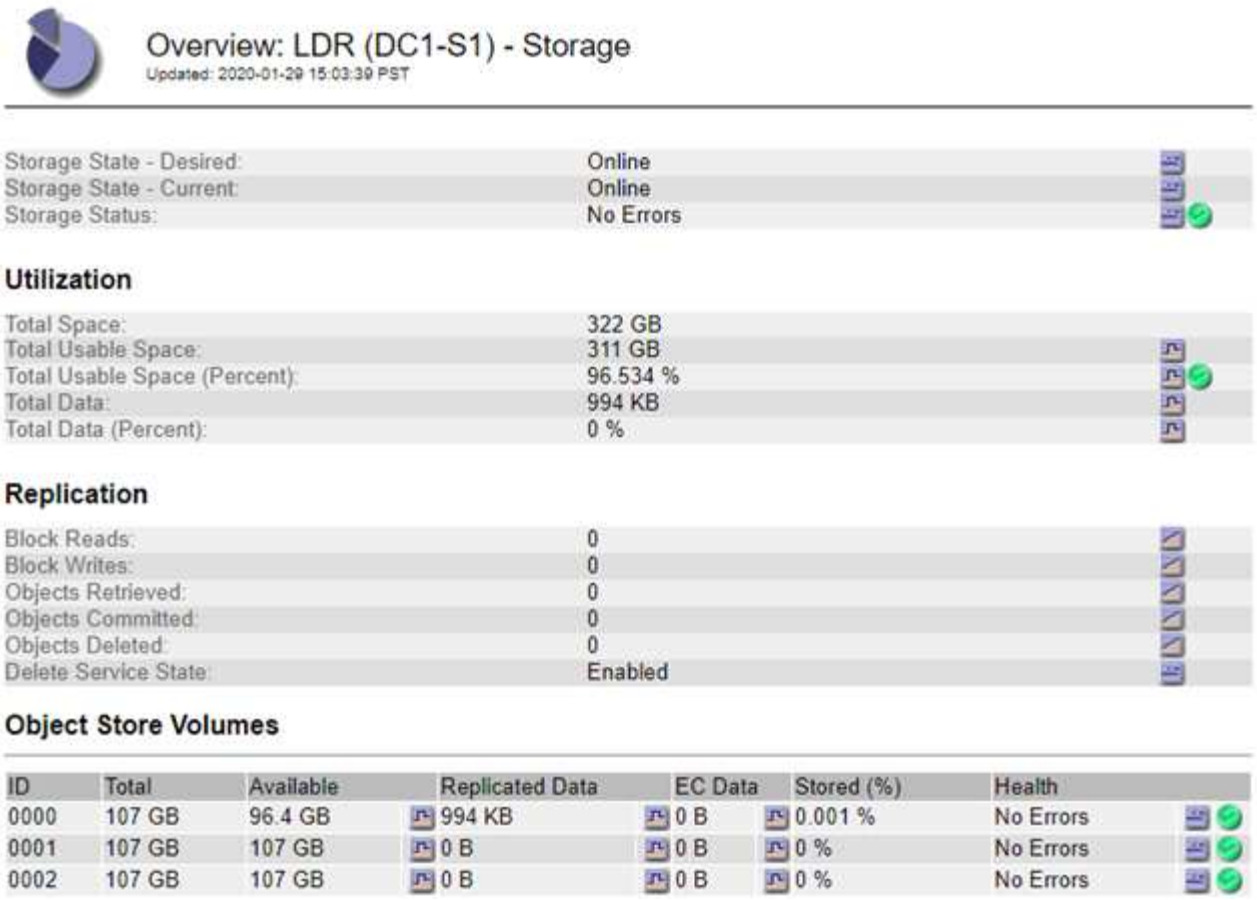
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Para ver mais detalhes sobre cada nó de storage, siga estas etapas:

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site Storage Node*** **LDR Storage Overview Main**.



Dependendo da natureza da falha, as falhas com um volume de armazenamento podem ser refletidas em um alarme sobre o status de armazenamento ou sobre a integridade de um armazenamento de objetos. Se um volume de armazenamento falhar, você deve reparar o volume de armazenamento com falha para restaurar o nó de armazenamento para a funcionalidade completa o mais rápido possível. Se necessário, você pode ir para a guia **Configuração** e colocar o nó de armazenamento em um estado somente leitura para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto se prepara para uma recuperação completa do servidor.

Informações relacionadas

"Manter recuperar"

Verificando a integridade do objeto

O sistema StorageGRID verifica a integridade dos dados de objetos nos nós de storage, verificando se há objetos corrompidos ou ausentes.

Existem dois processos de verificação: Verificação em segundo plano e verificação em primeiro plano. Eles trabalham juntos para garantir a integridade dos dados. A verificação em segundo plano é executada automaticamente e verifica continuamente a correção dos dados do objeto. A verificação de primeiro plano pode ser acionada por um usuário, para verificar mais rapidamente a existência (embora não a correção) de objetos.

O que é a verificação de antecedentes

O processo de verificação em segundo plano verifica automaticamente e continuamente os nós de storage em busca de cópias corrompidas de dados de objetos e tenta reparar automaticamente quaisquer problemas

encontrados.

A verificação em segundo plano verifica a integridade dos objetos replicados e dos objetos codificados por apagamento, da seguinte forma:

- **Objetos replicados**: Se o processo de verificação em segundo plano encontrar um objeto replicado que está corrompido, a cópia corrompida será removida de seu local e colocada em quarentena em outro lugar no nó de armazenamento. Em seguida, uma nova cópia não corrompida é gerada e colocada para satisfazer a política ILM ativa. A nova cópia pode não ser colocada no nó de armazenamento que foi usado para a cópia original.

> Os dados de objetos corrompidos são colocados em quarentena em vez de excluídos do sistema, para que ainda possam ser acessados. Para obter mais informações sobre como acessar dados de objetos em quarentena, entre em Contato com o suporte técnico.

- **Objetos codificados por apagamento**: Se o processo de verificação em segundo plano detetar que um fragmento de um objeto codificado por apagamento está corrompido, o StorageGRID tentará automaticamente reconstruir o fragmento ausente no mesmo nó de storage, usando os dados restantes e fragmentos de paridade. Se o fragmento corrompido não puder ser reconstruído, o atributo cópias corrompidas detetadas (ECOR) é incrementado por um, e uma tentativa é feita para recuperar outra cópia do objeto. Se a recuperação for bem-sucedida, uma avaliação ILM será executada para criar uma cópia de substituição do objeto codificado de apagamento.

  O processo de verificação em segundo plano verifica objetos apenas nos nós de storage. Ele não verifica objetos em nós de arquivamento ou em um pool de storage de nuvem. Os objetos devem ter mais de quatro dias para serem qualificados para verificação em segundo plano.

A verificação em segundo plano é executada a uma taxa contínua que é projetada para não interferir nas atividades comuns do sistema. A verificação em segundo plano não pode ser interrompida. No entanto, você pode aumentar a taxa de verificação em segundo plano para verificar mais rapidamente o conteúdo de um nó de armazenamento se suspeitar de um problema.

Alertas e alarmes (legacy) relacionados à verificação em segundo plano

Se o sistema detetar um objeto corrompido que não possa corrigir automaticamente (porque a corrupção impede que o objeto seja identificado), o alerta **Objeto corrompido não identificado detetado** é acionado.

Se a verificação em segundo plano não puder substituir um objeto corrompido porque ele não consegue localizar outra cópia, o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) são acionados.

Alterar a taxa de verificação em segundo plano

Você pode alterar a taxa na qual a verificação em segundo plano verifica os dados de objetos replicados em um nó de storage se tiver preocupações com a integridade dos dados.

O que você vai precisar

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

Sobre esta tarefa

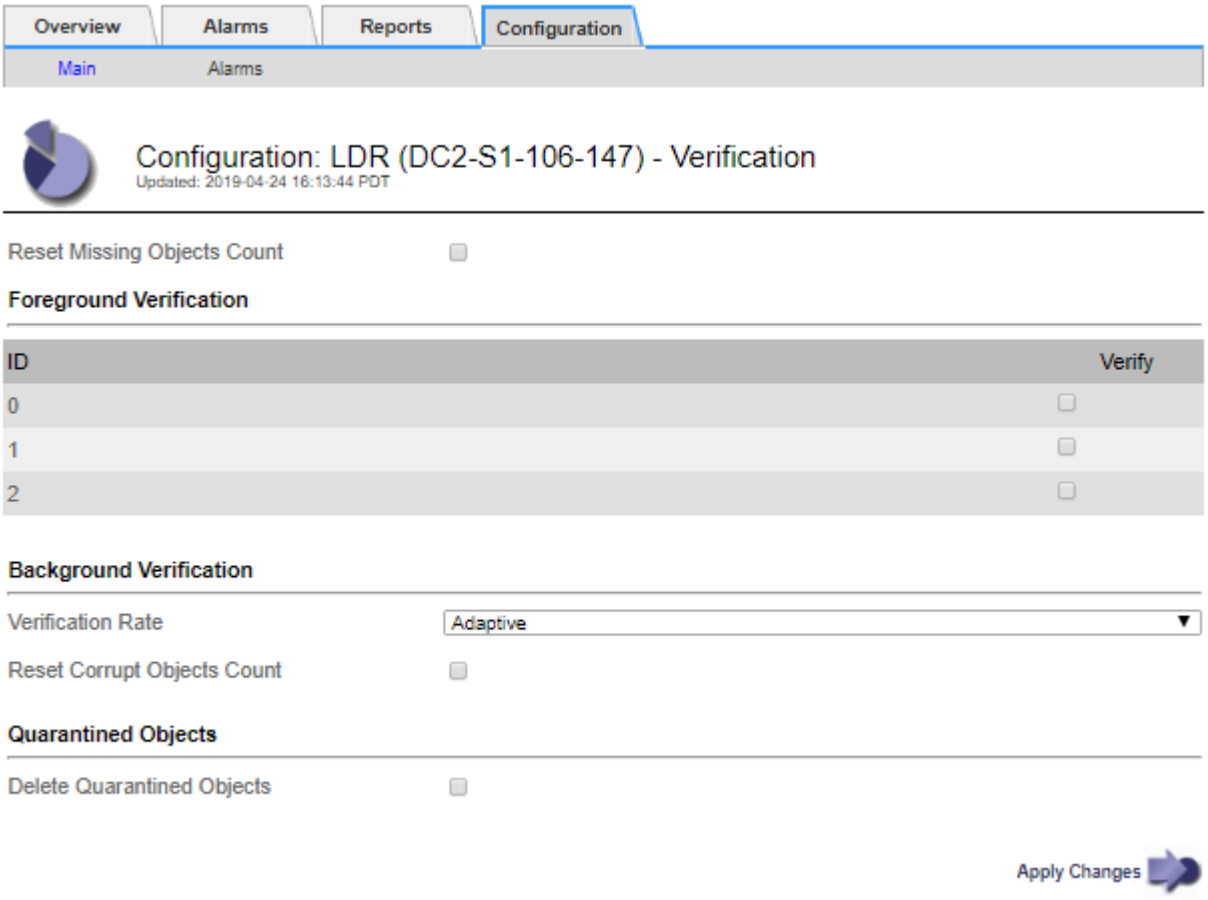
Você pode alterar a taxa de verificação para verificação em segundo plano em um nó de storage:

- Adaptive (adaptável): Predefinição. A tarefa foi projetada para verificar no máximo 4 MB/s ou 10 objetos/s (o que for excedido primeiro).
- Alta: A verificação do armazenamento prossegue rapidamente, a uma taxa que pode retardar as atividades normais do sistema.

Use a taxa de verificação alta somente quando suspeitar que uma falha de hardware ou software pode ter dados de objeto corrompidos. Após a conclusão da verificação de fundo de alta prioridade, a taxa de verificação é automaticamente redefinida para Adaptive (adaptável).

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Storage Node* LDR Verification**.
3. Selecione **Configuração** > **Principal**.
4. Vá para **LDR Verificação Configuração Principal**.
5. Em Verificação em segundo plano, selecione **taxa de verificação alta** ou **taxa de verificação adaptável**.



Definir a taxa de verificação como alta aciona o alarme legado VPRI (taxa de verificação) no nível de aviso.

1. Clique em **aplicar alterações**.
2. Monitore os resultados da verificação em segundo plano para objetos replicados.
   a. Vá para **nodes *Storage Node* Objects**.

b. Na seção Verificação, monitore os valores para **objetos corrompidos** e **objetos corrompidos não identificados**.

   Se a verificação em segundo plano encontrar dados de objeto replicados corrompidos, a métrica **objetos corrompidos** será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte forma:

   - Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar do sistema StorageGRID que satisfaça a política ILM ativa.
   - Se o identificador de objeto não puder ser extraído (porque foi corrompido), a métrica **objetos corrompidos não identificados** é incrementada e o alerta **Objeto corrompido não identificado detetado** é acionado.

c. Se forem encontrados dados de objeto replicados corrompidos, entre em Contato com o suporte técnico para determinar a causa raiz da corrupção.

3. Monitore os resultados da verificação em segundo plano para objetos codificados por apagamento.

   Se a verificação em segundo plano encontrar fragmentos corrompidos de dados de objetos codificados por apagamento, o atributo fragmentos corrompidos detetados é incrementado. O StorageGRID se recupera reconstruindo o fragmento corrompido no mesmo nó de storage.

   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***Storage Node*** **LDR Erasure Coding**.
   c. Na tabela resultados da verificação, monitore o atributo fragmentos corrompidos detetados (ECCD).

4. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID, redefina a contagem de objetos corrompidos.
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***Storage Node*** **LDR Verification Configuration**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **aplicar alterações**.
5. Se você estiver confiante de que objetos em quarentena não são necessários, você pode excluí-los.

> Se o alerta **objetos perdidos** ou o alarme legado PERDIDO (objetos perdidos) foi acionado, o suporte técnico pode querer acessar objetos em quarentena para ajudar a depurar o problema subjacente ou tentar a recuperação de dados.

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Storage Node*** **LDR Verificação Configuração**.
3. Selecione **Excluir objetos em quarentena**.
4. Clique em **aplicar alterações**.

O que é a verificação de primeiro plano

A verificação em primeiro plano é um processo iniciado pelo usuário que verifica se todos os dados de objeto esperados existem em um nó de armazenamento. A verificação de primeiro plano é usada para verificar a integridade de um dispositivo de armazenamento.

A verificação em primeiro plano é uma alternativa mais rápida à verificação em segundo plano que verifica a

existência, mas não a integridade, de dados de objetos em um nó de armazenamento. Se a verificação de primeiro plano descobrir que muitos itens estão faltando, pode haver um problema com a totalidade ou parte de um dispositivo de armazenamento associado ao nó de armazenamento.

A verificação em primeiro plano verifica os dados de objetos replicados e os dados de objetos codificados por apagamento, da seguinte forma:

- **Objetos replicados**: Se uma cópia dos dados de objetos replicados estiver ausente, o StorageGRID tentará substituir automaticamente a cópia de cópias armazenadas em outro lugar do sistema. O nó de armazenamento executa uma cópia existente através de uma avaliação ILM, que determinará que a política ILM atual não está mais sendo atendida para este objeto porque a cópia ausente não existe mais no local esperado. Uma nova cópia é gerada e colocada para satisfazer a política ILM ativa do sistema. Esta nova cópia pode não ser colocada no mesmo local em que a cópia em falta foi armazenada.
- **Objetos codificados por apagamento**: Se um fragmento de um objeto codificado por apagamento estiver ausente, o StorageGRID tentará reconstruir automaticamente o fragmento ausente no mesmo nó de armazenamento usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), o atributo cópias corrompidas detetadas (ECOR) é incrementado por um. O ILM então tenta encontrar outra cópia do objeto, que ele pode usar para gerar uma nova cópia codificada por apagamento.

  Se a verificação em primeiro plano identificar um problema com a codificação de apagamento em um volume de armazenamento, a tarefa de verificação em primeiro plano será interrompida com uma mensagem de erro que identifique o volume afetado. Você deve executar um procedimento de recuperação para todos os volumes de armazenamento afetados.

Se nenhuma outra cópia de um objeto replicado em falta ou de um objeto codificado de apagamento corrompido puder ser encontrada na grade, o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) serão acionados.

A executar a verificação de primeiro plano

A verificação em primeiro plano permite verificar a existência de dados em um nó de armazenamento. Dados de objeto ausentes podem indicar que existe um problema com o dispositivo de armazenamento subjacente.

O que você vai precisar

- Você garantiu que as seguintes tarefas de grade não estão sendo executadas:
  - Expansão da grade: Adicione servidor (GEXP), ao adicionar um nó de armazenamento
  - Desativação do nó de armazenamento (LDCM) no mesmo nó de armazenamento se estas tarefas de grade estiverem em execução, aguarde que elas sejam concluídas ou liberem seu bloqueio.
- Você garantiu que o armazenamento está online. (Selecione **Support Tools Grid Topology**. Em seguida, selecione ***Storage Node* LDR Storage Overview Main**. Certifique-se de que **Estado de armazenamento - atual** está online.)
- Você garantiu que os seguintes procedimentos de recuperação não estão sendo executados no mesmo nó de storage:
  - Recuperação de um volume de armazenamento com falha
  - A recuperação de um nó de armazenamento com uma falha na verificação de primeiro plano da unidade do sistema não fornece informações úteis enquanto os procedimentos de recuperação estão em andamento.

Sobre esta tarefa

Verificações de primeiro plano para dados de objetos replicados em falta e dados de objetos codificados por

apagamento em falta:

- Se a verificação em primeiro plano encontrar grandes quantidades de dados de objetos em falta, provavelmente há um problema com o armazenamento do nó de armazenamento que precisa ser investigado e resolvido.
- Se a verificação em primeiro plano encontrar um erro de armazenamento grave associado a dados codificados por apagamento, ela o notificará. Você deve executar a recuperação do volume de armazenamento para reparar o erro.

Você pode configurar a verificação de primeiro plano para verificar todos os armazenamentos de objetos de um nó de armazenamento ou apenas armazenamentos de objetos específicos.

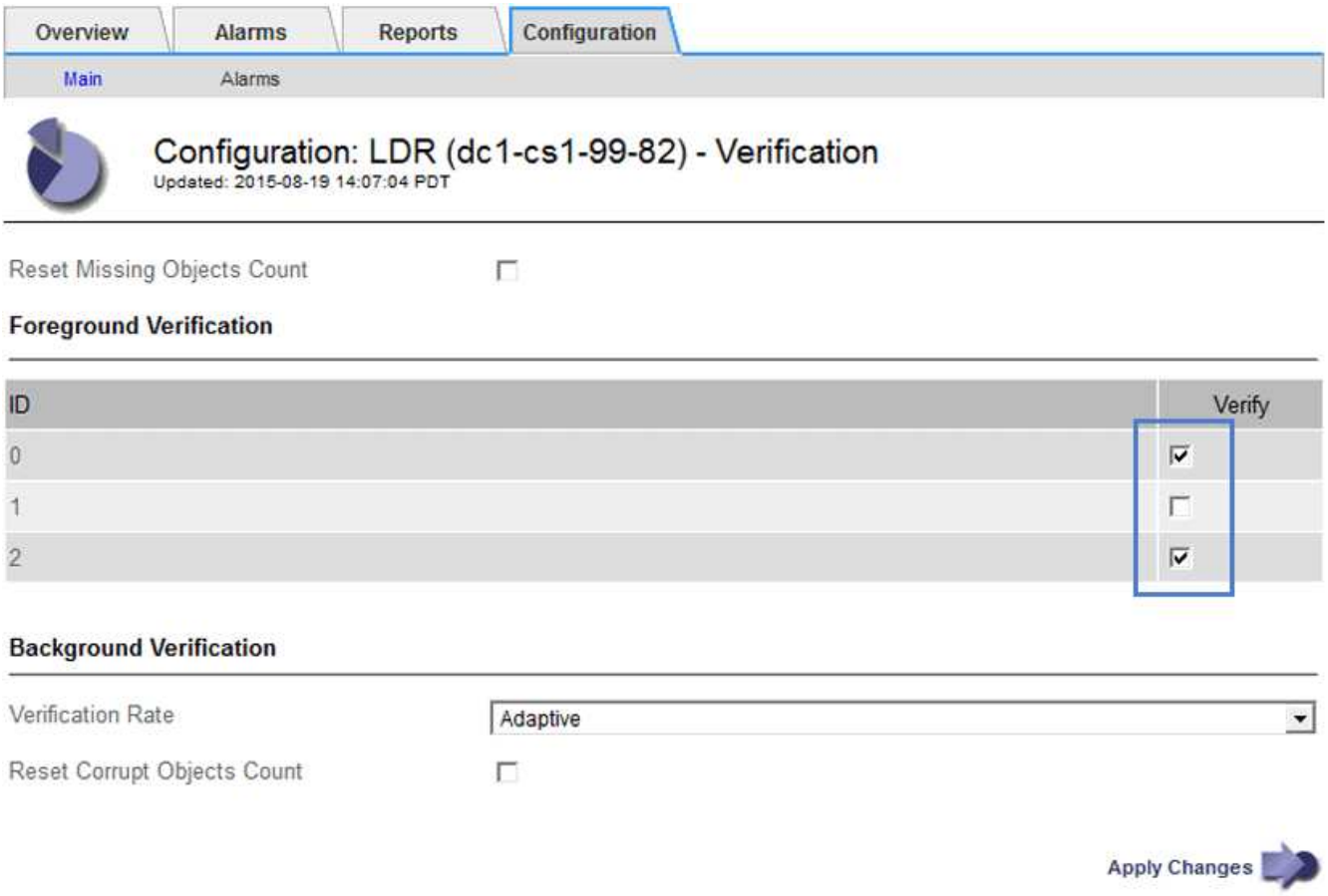
Se a verificação de primeiro plano encontrar dados de objeto em falta, o sistema StorageGRID tentará substituí-los. Se não for possível efetuar uma cópia de substituição, o alarme PERDIDO (objetos perdidos) poderá ser acionado.

A verificação em primeiro plano gera uma tarefa de grade de verificação em primeiro plano LDR que, dependendo do número de objetos armazenados em um nó de armazenamento, pode levar dias ou semanas para ser concluída. É possível selecionar vários nós de storage ao mesmo tempo; no entanto, essas tarefas de grade não são executadas simultaneamente. Em vez disso, eles são enfileirados e executados um após o outro até a conclusão. Quando a verificação em primeiro plano está em andamento em um nó de armazenamento, você não pode iniciar outra tarefa de verificação em primeiro plano nesse mesmo nó de armazenamento, mesmo que a opção para verificar volumes adicionais possa parecer estar disponível para o nó de armazenamento.

Se um nó de armazenamento diferente daquele em que a verificação de primeiro plano está sendo executada ficar off-line, a tarefa de grade continuará sendo executada até que o atributo **% completo** atinja 99,99%. O atributo **% complete** então volta para 50 por cento e espera que o nó de armazenamento retorne ao status online. Quando o estado do nó de armazenamento regressa à linha, a tarefa da grelha de verificação de primeiro plano do LDR continua até ser concluída.

Passos

1. Selecione ***Storage Node* LDR Verification**.
2. Selecione **Configuração** > **Principal**.
3. Em **Verificação de primeiro plano**, marque a caixa de seleção para cada ID de volume de armazenamento que deseja verificar.



4. Clique em **aplicar alterações**.

   Aguarde até que a página seja atualizada automaticamente e recarregada antes de sair da página. Uma vez atualizados, os armazenamentos de objetos ficam indisponíveis para seleção nesse nó de armazenamento.

   Uma tarefa de grade de verificação de primeiro plano do LDR é gerada e executada até que ela seja concluída, pausa ou abortada.

5. Monitorar objetos em falta ou fragmentos em falta:

   a. Selecione ***Storage Node* LDR Verification**.

   b. Na guia Visão geral em **resultados da verificação**, observe o valor de **objetos ausentes detetados**.

      Nota: O mesmo valor é relatado como **objetos perdidos** na página de nós. Vá para **nodes *Storage Node*** e selecione a guia **Objects**.

      Se o número de **objetos ausentes detetados** for grande (se houver centenas de objetos ausentes), provavelmente há um problema com o armazenamento do nó de armazenamento. Entre em Contato com o suporte técnico.

   c. Selecione ***Storage Node* LDR Erasure Coding**.

   d. Na guia Visão geral em **resultados da verificação**, observe o valor de **fragmentos ausentes detetados**.

      Se o número de **fragmentos ausentes detetados** for grande (se houver centenas de fragmentos ausentes), provavelmente há um problema com o armazenamento do nó de armazenamento. Entre

em Contato com o suporte técnico.

Se a verificação em primeiro plano não detetar um número significativo de cópias de objetos replicados em falta ou um número significativo de fragmentos ausentes, o storage estará operando normalmente.

6. Monitorize a conclusão da tarefa de grelha de verificação em primeiro plano:
   a. Selecione **Support Tools Grid Topology**. Em seguida, selecione **site *Admin Node* CMN Grid Task Overview Main**.
   b. Verifique se a tarefa da grade de verificação de primeiro plano está progredindo sem erros.

      Nota: Um alarme de nível de aviso é acionado no status da tarefa de grade (SCAs) se a tarefa de grade de verificação de primeiro plano for interrompida.

   c. Se a tarefa de grade parar com um `critical storage error`, recupere o volume afetado e execute a verificação de primeiro plano nos volumes restantes para verificar se há erros adicionais.

      Atenção: Se a tarefa da grade de verificação de primeiro plano for interrompida com a mensagem `Encountered a critical storage error in volume volID`, você deverá executar o procedimento para recuperar um volume de armazenamento com falha. Consulte as instruções de recuperação e manutenção.

Depois de terminar

Se você ainda tiver dúvidas sobre a integridade dos dados, vá para **LDR Verificação Configuração Principal** e aumente a taxa de Verificação em segundo plano. A verificação em segundo plano verifica a exatidão de todos os dados de objetos armazenados e repara quaisquer problemas que encontrar. Encontrar e reparar possíveis problemas o mais rápido possível reduz o risco de perda de dados.

Informações relacionadas

"Manter recuperar"

Solução de problemas de dados de objetos perdidos e ausentes

Os objetos podem ser recuperados por vários motivos, incluindo solicitações de leitura de um aplicativo cliente, verificações em segundo plano de dados de objeto replicados, reavaliações ILM e a restauração de dados de objeto durante a recuperação de um nó de armazenamento.

O sistema StorageGRID usa informações de localização nos metadados de um objeto para determinar a partir de qual local recuperar o objeto. Se uma cópia do objeto não for encontrada no local esperado, o sistema tentará recuperar outra cópia do objeto de outra parte do sistema, assumindo que a política ILM contém uma regra para fazer duas ou mais cópias do objeto.

Se esta recuperação for bem-sucedida, o sistema StorageGRID substitui a cópia em falta do objeto. Caso contrário, o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) são acionados, da seguinte forma:

- Para cópias replicadas, se outra cópia não puder ser recuperada, o objeto será considerado perdido e o alerta e o alarme serão disparados.
- Para cópias codificadas de apagamento, se uma cópia não puder ser recuperada do local esperado, o atributo cópias corrompidas detetadas (ECOR) é incrementado por um antes de uma tentativa ser feita

para recuperar uma cópia de outro local. Se não for encontrada outra cópia, o alerta e o alarme são acionados.

Você deve investigar todos os alertas de **objetos perdidos** imediatamente para determinar a causa raiz da perda e determinar se o objeto ainda pode existir em um nó de armazenamento ou nó de arquivo offline, ou de outra forma atualmente indisponível.

No caso de perda de dados de objetos sem cópias, não há solução de recuperação. No entanto, você deve redefinir o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos.

Informações relacionadas

"Investigando objetos perdidos"

"Repor contagens de objetos perdidas e em falta"

Investigando objetos perdidos

Quando o alerta **objetos perdidos** e o alarme legado PERDIDO (objetos perdidos) são acionados, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em Contato com o suporte técnico.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

O alerta **objetos perdidos** e o alarme PERDIDO indicam que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

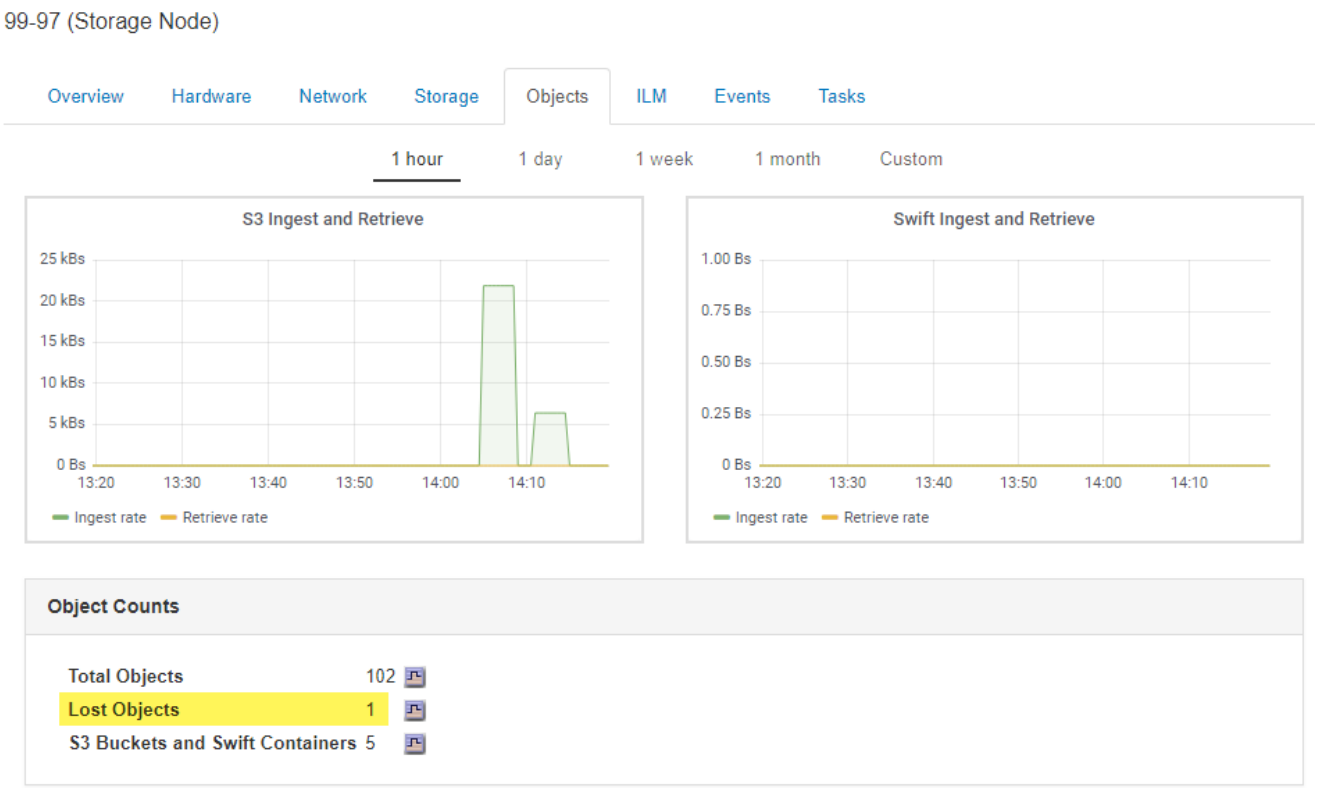
Investigue alarmes ou alertas de objetos perdidos imediatamente. Talvez seja necessário tomar medidas para evitar mais perda de dados. Em alguns casos, você pode restaurar um objeto perdido se você tomar uma ação imediata.

O número de objetos perdidos pode ser visto no Gerenciador de Grade.

Passos

1. Selecione **nós**.
2. Selecione ***Storage Node* Objects**.
3. Revise o número de objetos perdidos mostrados na tabela contagens de objetos.

   Esse número indica o número total de objetos que esse nó de grade deteta como ausente de todo o sistema StorageGRID. O valor é a soma dos contadores de objetos perdidos do componente armazenamento de dados nos serviços LDR e DDS.



4. A partir de um nó Admin, acesse o log de auditoria para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **objetos perdidos** e o alarme PERDIDO:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Mude para o diretório onde os logs de auditoria estão localizados. Introduza: `cd /var/local/audit/export/`
   c. Use grep para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`
   d. Observe o valor UUID incluído na mensagem.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Use o `ObjectByUUID` comando para encontrar o objeto pelo seu identificador (UUID) e, em seguida, determinar se os dados estão em risco.

   a. Telnet para localhost 1402 para acessar o console LDR.

   b. Introduza: `/proc/OBRP/ObjectByUUID UUID_value`

      Neste primeiro exemplo, o objeto com `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` tem duas localizações listadas.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
```

```
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

No segundo exemplo, o objeto com `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` não tem locais listados.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Revise a saída de /proc/OBRP/ObjectByUID e tome a ação apropriada:

Metadados	Conclusão
Nenhum objeto encontrado ("ERRO":"")	Se o objeto não for encontrado, a mensagem "ERROR":" é retornada. Se o objeto não for encontrado, é seguro ignorar o alarme. A falta de um objeto indica que o objeto foi intencionalmente excluído.
Locais 0	Se houver locais listados na saída, o alarme de objetos perdidos pode ser um falso positivo. Confirme se os objetos existem. Use o ID do nó e o filepath listados na saída para confirmar se o arquivo de objeto está no local listado. (O procedimento para localizar objetos potencialmente perdidos explica como usar o ID do nó para encontrar o nó de armazenamento correto.) "Procurar e restaurar objetos potencialmente perdidos" Se existirem objetos, pode repor a contagem de objetos perdidos para limpar o alarme e o alerta.
Localização: 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar encontrar e restaurar o objeto você mesmo, ou você pode entrar em Contato com o suporte técnico. "Procurar e restaurar objetos potencialmente perdidos" O suporte técnico pode pedir-lhe para determinar se existe um procedimento de recuperação de armazenamento em curso. Ou seja, um comando *repair-data* foi emitido em qualquer nó de armazenamento e a recuperação ainda está em andamento? Consulte as informações sobre como restaurar dados de objetos para um volume de armazenamento nas instruções de recuperação e manutenção.

Informações relacionadas

"Manter recuperar"

"Rever registos de auditoria"

Procurar e restaurar objetos potencialmente perdidos

Pode ser possível encontrar e restaurar objetos que acionaram um alarme de objetos perdidos (PERDIDOS) e um alerta **Objeto perdido** e que você identificou como potencialmente perdido.

O que você vai precisar

- Você deve ter o UUID de qualquer objeto perdido, conforme identificado em "investigando objetos perdidos".
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Você pode seguir este procedimento para procurar cópias replicadas do objeto perdido em outro lugar na grade. Na maioria dos casos, o objeto perdido não será encontrado. No entanto, em alguns casos, você pode encontrar e restaurar um objeto replicado perdido se você executar uma ação de prompt.

Contacte o suporte técnico para obter assistência com este procedimento.

Passos

1. A partir de um nó Admin, procure os logs de auditoria para possíveis localizações de objetos:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/audit/export/`
   c. Use o grep para extrair as mensagens de auditoria associadas ao objeto potencialmente perdido e enviá-las para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

      Por exemplo:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Use grep para extrair as mensagens de auditoria de localização perdida (LLST) deste arquivo de saída. Introduza: `grep LLST output_file_name`

      Por exemplo:

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      Uma mensagem de auditoria LLST se parece com essa mensagem de exemplo.

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. Localize o campo PCLD e o campo NOID na mensagem LLST.

Se presente, o valor de PCLD é o caminho completo no disco para a cópia de objeto replicado em falta. O valor de NOID é o id do nó do LDR onde uma cópia do objeto pode ser encontrada.

Se você encontrar um local de objeto, poderá restaurar o objeto.

f. Localize o nó de armazenamento para este ID de nó LDR.

Há duas maneiras de usar o ID do nó para localizar o nó de storage:

- No Gerenciador de Grade, selecione **suporte Ferramentas topologia de Grade**. Em seguida, selecione ***Data Center Storage Node* LDR**. O ID do nó LDR está na tabela informações do nó. Reveja as informações de cada nó de armazenamento até encontrar o que hospeda este LDR.
- Baixe e descompacte o Pacote de recuperação para a grade. Existe um diretório *_docs* no REFERIDO pacote. Se você abrir o arquivo index.html, o Resumo de servidores mostrará todas as IDs de nó para todos os nós de grade.

2. Determine se o objeto existe no nó de armazenamento indicado na mensagem de auditoria:

a. Faça login no nó da grade:

i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

b. Determine se o caminho do arquivo para o objeto existe.

Para o caminho do arquivo do objeto, use o valor de PCLD da mensagem de auditoria LLST.

Por exemplo, digite:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Nota: Sempre inclua o caminho do arquivo de objeto em aspas simples em comandos para escapar de quaisquer carateres especiais.

- Se o caminho do objeto não for encontrado, o objeto é perdido e não pode ser restaurado usando

este procedimento. Entre em Contato com o suporte técnico.

- Se o caminho do objeto for encontrado, continue com a Restaure o objeto para o StorageGRIDetapa . Você pode tentar restaurar o objeto encontrado de volta para o StorageGRID.

1. Se o caminho do objeto foi encontrado, tente restaurar o objeto para StorageGRID:
   a. No mesmo nó de storage, altere a propriedade do arquivo de objeto para que ele possa ser gerenciado pelo StorageGRID. Introduza: `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet para localhost 1402 para acessar o console LDR. Introduza: `telnet 0 1402`
   c. Introduza: `cd /proc/STOR`
   d. Introduza: `Object_Found 'file_path_of_object'`

      Por exemplo, digite:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      A emissão do `Object\_Found` comando notifica a grade da localização do objeto. Ele também aciona a política ILM ativa, que faz cópias adicionais conforme especificado na política.

      Nota: Se o nó de armazenamento onde você encontrou o objeto estiver offline, você poderá copiar o objeto para qualquer nó de armazenamento que esteja online. Coloque o objeto em qualquer diretório /var/local/rangedb do nó de armazenamento online. Em seguida, emita o `Object\_Found` comando usando esse caminho de arquivo para o objeto.

      - Se o objeto não puder ser restaurado, o `Object\_Found` comando falhará. Entre em Contato com o suporte técnico.
      - Se o objeto foi restaurado com sucesso para o StorageGRID, uma mensagem de sucesso será exibida. Por exemplo:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Avance para o passo Verifique se foram criados novos locais

1. Se o objeto foi restaurado com sucesso para o StorageGRID, verifique se novos locais foram criados.
   a. Introduza: `cd /proc/OBRP`
   b. Introduza: `ObjectByUUID UUID_value`

      O exemplo a seguir mostra que há dois locais para o objeto com UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
```

```
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Saia da consola LDR. Introduza: `exit`

2. Em um nó Admin, pesquise os logs de auditoria para a mensagem de auditoria ORLM para este objeto para confirmar que o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme necessário.

   a. Faça login no nó da grade:

      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      iii. Digite o seguinte comando para mudar para root: `su -`

      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

   b. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/audit/export/`

   c. Use grep para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

      Por exemplo:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_restored_object.txt
      ```

   d. Use o grep para extrair as mensagens de auditoria regras de objeto atendidas (ORLM) deste arquivo de saída. Introduza: `grep ORLM output_file_name`

      Por exemplo:

      ```
      Admin: # grep ORLM messages_about_restored_object.txt
      ```

      Uma mensagem de auditoria ORLM se parece com essa mensagem de exemplo.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Localize o campo LOCS na mensagem de auditoria.

   Se presente, o valor de CLDI em LOCS é o ID do nó e o ID do volume onde uma cópia de objeto foi criada. Esta mensagem mostra que o ILM foi aplicado e que duas cópias de objeto foram criadas em dois locais na grade.

b. Redefina a contagem de objetos perdidos no Gerenciador de Grade.

Informações relacionadas

"Investigando objetos perdidos"

"Confirmar localizações de dados do objeto"

"Repor contagens de objetos perdidas e em falta"

"Rever registos de auditoria"

Repor contagens de objetos perdidas e em falta

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos gravados são perdidos permanentemente ou se é um alarme falso, você pode redefinir o valor do atributo objetos perdidos para zero.

O que você vai precisar

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

Sobre esta tarefa

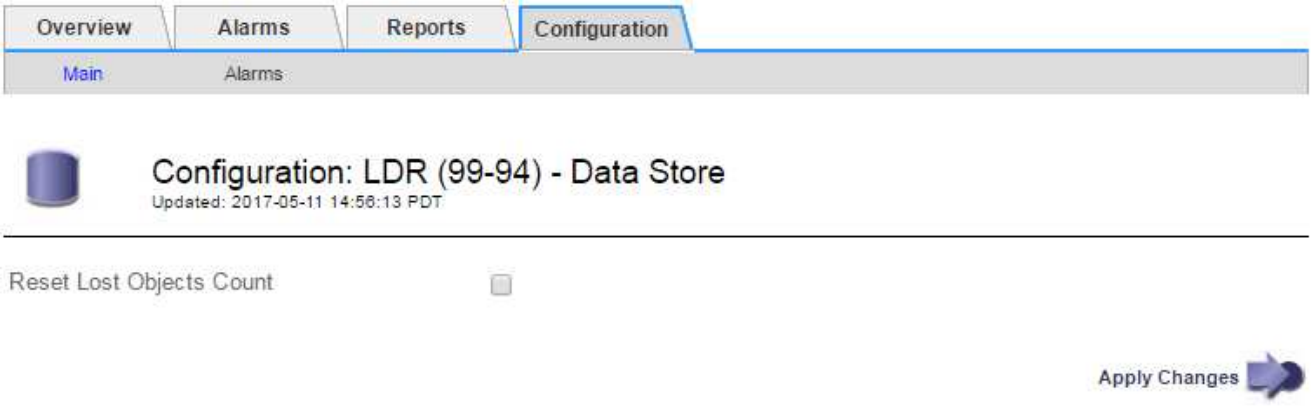
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

- **Suporte Ferramentas topologia de Grade *Site Storage Node* LDR Data Store Overview Main**
- **Suporte Ferramentas topologia de Grade *Site Storage Node* DDS Data Store Visão geral Principal**

Estas instruções mostram a reposição do contador a partir da página **LDR Data Store**.

Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Site Storage Node* LDR Data Store Configuration** para o nó de armazenamento que tem o alerta **objetos perdidos** ou o alarme PERDIDO.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **aplicar alterações**.

   O atributo objetos perdidos é redefinido para 0 e o alerta **objetos perdidos** e o alarme PERDIDO são apagados, o que pode levar alguns minutos.

5. Opcionalmente, redefina outros valores de atributo relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.

   a. Selecione ***Site Storage Node*** **LDR Erasure Coding Configuration**.

   b. Selecione **Redefinir leituras de contagem de falhas** e **Redefinir cópias corrompidas detetadas contagem**.

   c. Clique em **aplicar alterações**.

   d. Selecione ***Site Storage Node*** **LDR Verificação Configuração**.

   e. Selecione **Redefinir contagem de objetos ausentes** e **Redefinir contagem de objetos corrompidos**.

   f. Se você tiver certeza de que objetos em quarentena não são necessários, selecione **Excluir objetos em quarentena**.

      Objetos em quarentena são criados quando a verificação em segundo plano identifica uma cópia de objeto replicado corrompido. Na maioria dos casos, o StorageGRID substitui automaticamente o objeto corrompido e é seguro excluir os objetos em quarentena. No entanto, se o alerta **objetos perdidos** ou o alarme PERDIDO for acionado, o suporte técnico pode querer acessar os objetos em quarentena.

   g. Clique em **aplicar alterações**.

   Pode demorar alguns momentos para que os atributos sejam redefinidos depois de clicar em **Apply Changes** (aplicar alterações).

Informações relacionadas

"Administrar o StorageGRID"

Solução de problemas do alerta de armazenamento de dados de objetos baixos

O alerta **armazenamento de dados de objeto baixo** monitora quanto espaço está disponível para armazenar dados de objeto em cada nó de armazenamento.

O que você vai precisar

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

Sobre esta tarefa

O **armazenamento de dados de objeto baixo** é acionado quando a quantidade total de dados de objeto codificados replicados e apagados em um nó de armazenamento atende a uma das condições configuradas na regra de alerta.

Por padrão, um alerta principal é acionado quando essa condição é avaliada como verdadeira:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Nesta condição:

- `storagegrid_storage_utilization_data_bytes` É uma estimativa do tamanho total dos dados de objetos codificados de apagamento e replicados para um nó de storage.
- `storagegrid_storage_utilization_usable_space_bytes` É a quantidade total de espaço de storage de objetos restante para um nó de storage.

Se um alerta maior ou menor **armazenamento de dados de objeto baixo** for acionado, você deve executar um procedimento de expansão o mais rápido possível.

Passos

1. Selecione **Alertas atual**.

   A página Alertas é exibida.

2. Na tabela de alertas, expanda o grupo de alertas **armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja exibir.

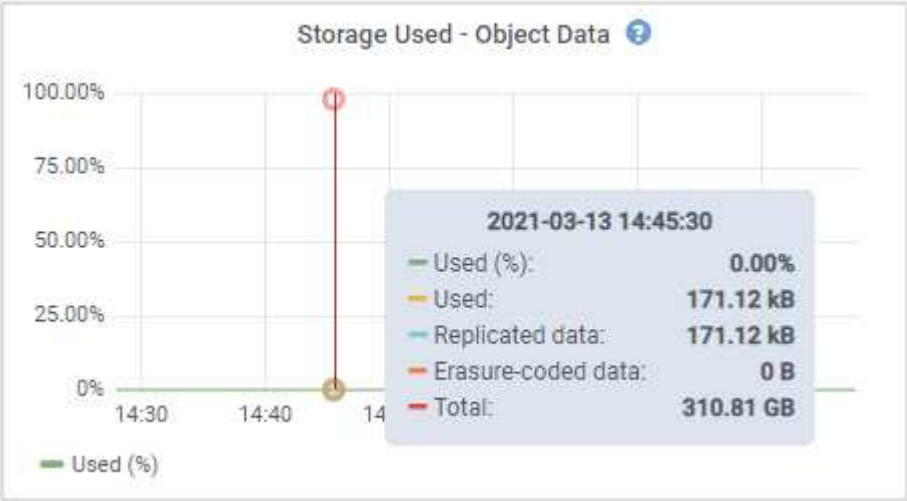
   Selecione o alerta e não o cabeçalho de um grupo de alertas.

3. Revise os detalhes na caixa de diálogo e observe o seguinte:
   - Tempo acionado
   - O nome do site e do nó
   - Os valores atuais das métricas para este alerta
4. Selecione **nós *Storage Node ou Site* Storage**.
5. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados do objeto).

   São apresentados os seguintes valores:

   - **Usado (%)**: A porcentagem do espaço utilizável total que foi usado para dados do objeto.
   - **Usado**: A quantidade de espaço utilizável total que foi usado para dados de objeto.
   - **Dados replicados**: Uma estimativa da quantidade de dados de objetos replicados neste nó, site ou grade.

- **Dados codificados por apagamento**: Uma estimativa da quantidade de dados de objetos codificados por apagamento neste nó, site ou grade.
- **Total**: A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é a `storagegrid_storage_utilization_data_bytes` métrica.



6. Selecione os controles de tempo acima do gráfico para exibir o uso do armazenamento em diferentes períodos de tempo.

   Analisar o uso do armazenamento ao longo do tempo pode ajudá-lo a entender quanto armazenamento foi usado antes e depois do alerta ser acionado e pode ajudá-lo a estimar quanto tempo pode levar para que o espaço restante do nó fique cheio.

7. Assim que possível, execute um procedimento de expansão para adicionar capacidade de armazenamento.

   Você pode adicionar volumes de storage (LUNs) aos nós de storage existentes ou adicionar novos nós de storage.

   > Para gerenciar um nó de storage completo, consulte as instruções de administração do StorageGRID.

Informações relacionadas

"Resolução de problemas do alarme de Estado de armazenamento (SSTS)"

"Expanda sua grade"

"Administrar o StorageGRID"

Resolução de problemas do alarme de Estado de armazenamento (SSTS)

O alarme de Estado de armazenamento (SSTS) é acionado se um nó de armazenamento tiver espaço livre insuficiente restante para armazenamento de objetos.

O que você vai precisar

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

Sobre esta tarefa

O alarme SSTS (Storage Status) é acionado no nível de Aviso quando a quantidade de espaço livre em cada volume em um nó de armazenamento cai abaixo do valor do volume de armazenamento Soft Read Only Watermark (**Configuração Opções de armazenamento Visão geral**).

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

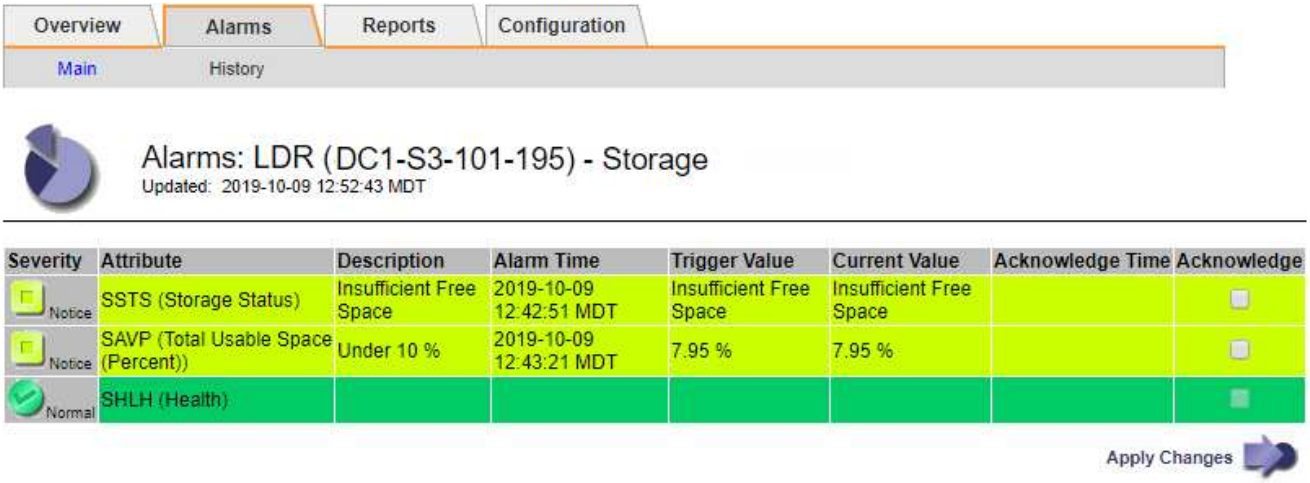
Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. O alarme SSTS é acionado se menos de 10 GB de espaço utilizável permanecer em cada volume de armazenamento no nó de armazenamento. Se algum dos volumes tiver 10 GB ou mais de espaço disponível, o alarme não será acionado.

Se um alarme SSTS tiver sido acionado, você pode seguir estes passos para entender melhor o problema.

Passos

1. Selecione **suporte Alarmes (legado) Alarmes atuais**.
2. Na coluna Serviço, selecione o data center, o nó e o serviço associados ao alarme SSTS.

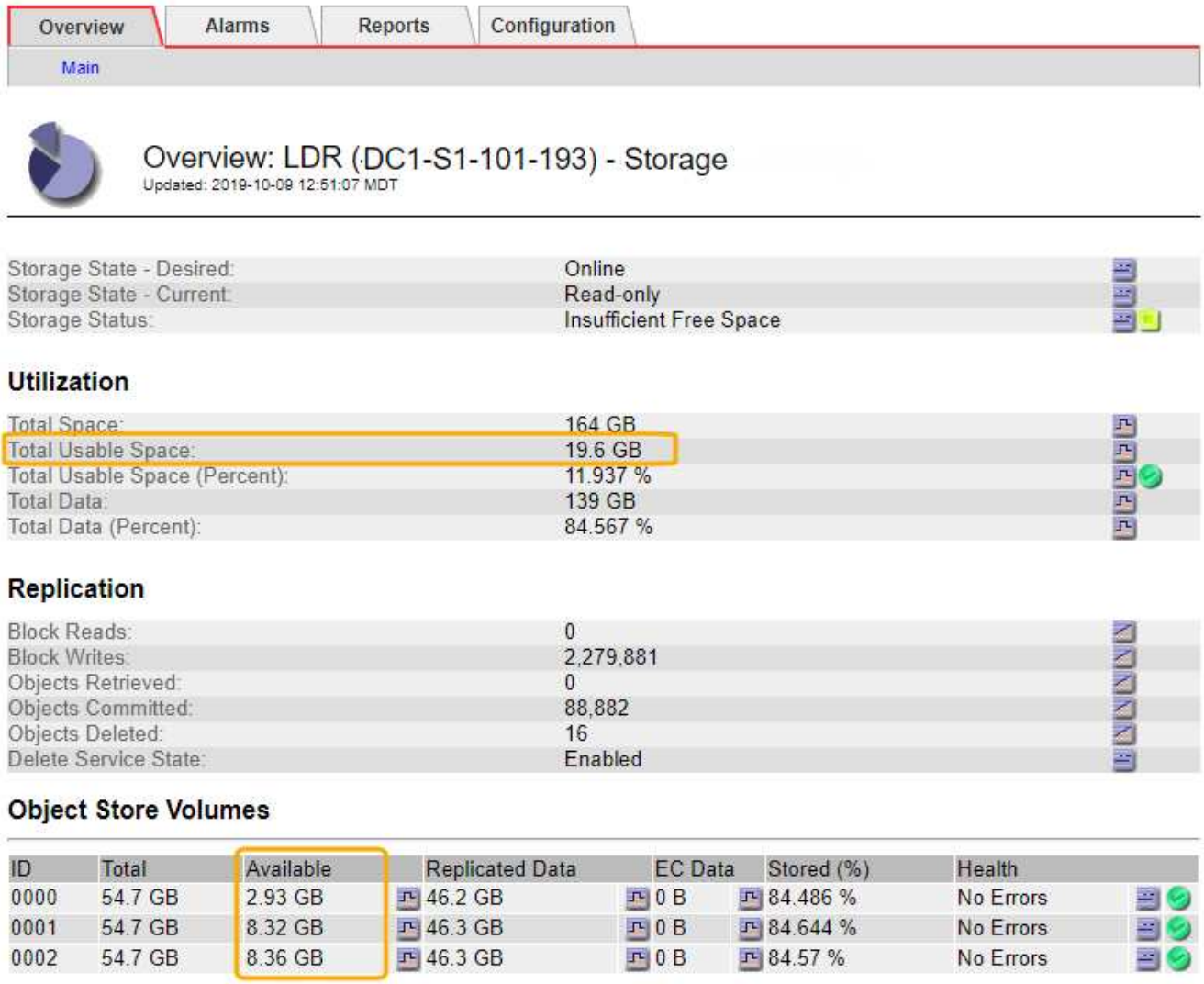
   É apresentada a página Grid Topology (topologia de grelha). A guia Alarmes mostra os alarmes ativos para o nó e serviço selecionados.



Neste exemplo, os alarmes SSTS (Storage Status) e SAVP (Total usable Space (Percent)) foram acionados no nível de Aviso.

> Normalmente, tanto o alarme SSTS como o alarme SAVP são acionados aproximadamente ao mesmo tempo; no entanto, se ambos os alarmes são acionados depende da definição da marca d'água em GB e da definição do alarme SAVP em percentagem.

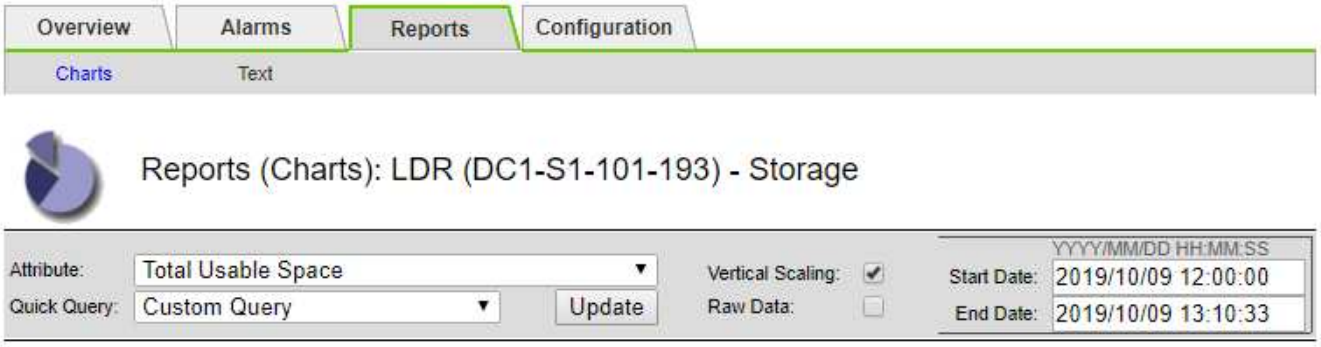
3. Para determinar quanto espaço utilizável está realmente disponível, selecione **LDR Storage Overview** e encontre o atributo espaço utilizável total (STAS).

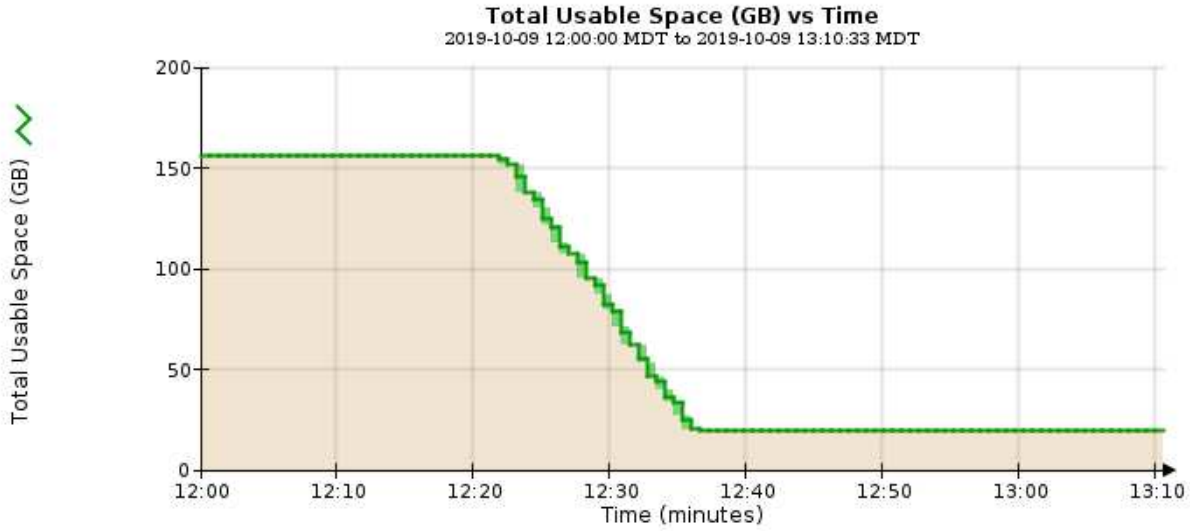


Neste exemplo, apenas 19,6 GB dos 164 GB de espaço neste nó de armazenamento permanecem disponíveis. Observe que o valor total é a soma dos valores **disponíveis** para os três volumes de armazenamento de objetos. O alarme SSTS foi acionado porque cada um dos três volumes de armazenamento tinha menos de 10 GB de espaço disponível.

4. Para entender como o armazenamento foi usado ao longo do tempo, selecione a guia **relatórios** e plote o espaço utilizável total nas últimas horas.

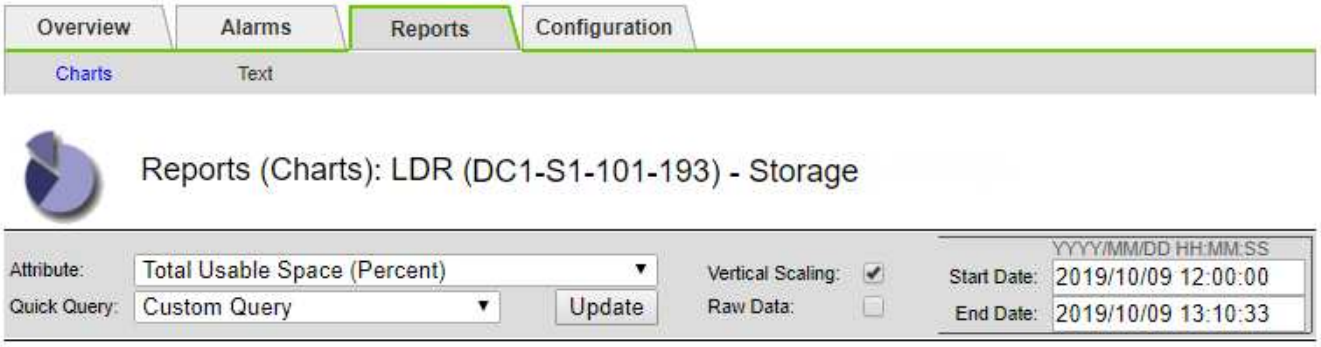
   Neste exemplo, o espaço utilizável total caiu de cerca de 155 GB em 12:00 para 20 GB em 12:35, o que corresponde ao momento em que o alarme SSTS foi acionado.

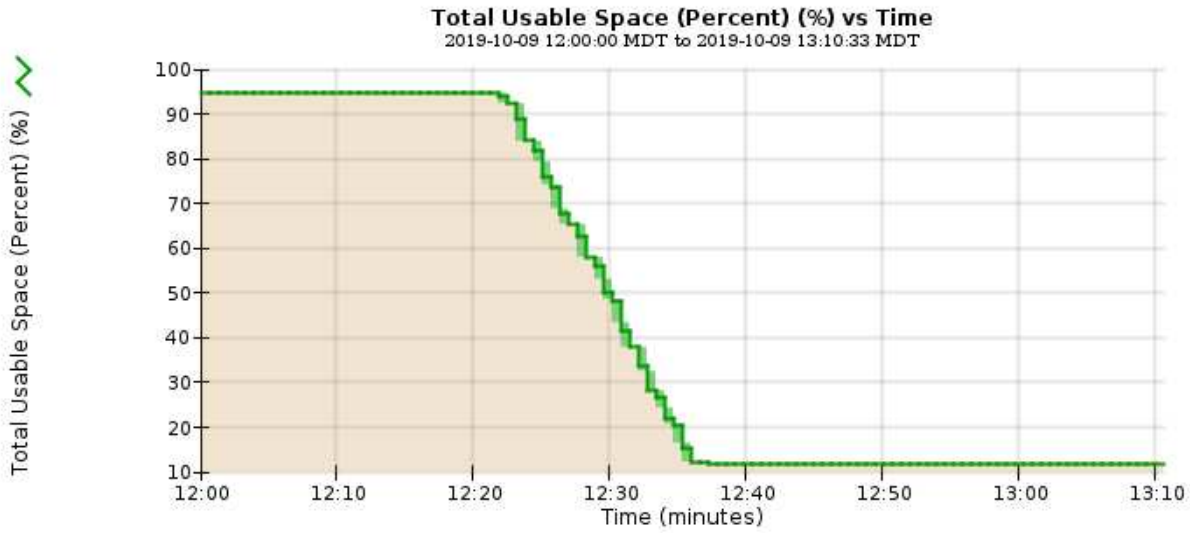




5. Para entender como o armazenamento está sendo usado como uma porcentagem do total, plote o espaço utilizável total (porcentagem) nas últimas horas.

   Neste exemplo, o espaço utilizável total caiu de 95% para pouco mais de 10%, aproximadamente ao mesmo tempo.





6. Conforme necessário, adicione capacidade de storage expandindo o sistema StorageGRID.

   Para obter procedimentos sobre como gerenciar um nó de armazenamento completo, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Expanda sua grade"

"Administrar o StorageGRID"

Solução de problemas de entrega de mensagens de serviços da plataforma (alarme SMTT)

O alarme Total Events (SMTT) é acionado no Grid Manager se uma mensagem de serviço da plataforma for entregue a um destino que não possa aceitar os dados.

Sobre esta tarefa

Por exemplo, um upload multipart S3 pode ser bem-sucedido, mesmo que a replicação ou a mensagem de notificação associada não possa ser entregue ao endpoint configurado. Ou, uma mensagem para replicação do CloudMirror pode não ser entregue se os metadados forem muito longos.

O alarme SMTT contém uma mensagem de último evento que diz, `Failed to publish notifications for bucket-name object key` para o último objeto cuja notificação falhou.

Para obter informações adicionais sobre os serviços de plataforma de solução de problemas, consulte as instruções de administração do StorageGRID. Talvez seja necessário acessar o locatário do Gerenciador do Locatário para depurar um erro de serviço de plataforma.

Passos

1. Para visualizar o alarme, selecione **nós *site grid node* Eventos**.
2. Veja o último evento na parte superior da tabela.

   As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

3. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
4. Clique em **Redefinir contagens de eventos**.
5. Notificar o locatário dos objetos cujas mensagens de serviços da plataforma não foram entregues.
6. Instrua o locatário a acionar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Referência de ficheiros de registo"

"Repor contagens de eventos"

Informações sobre direitos autorais

Informações sobre marcas comerciais