Solucionar problemas de objetos e storage

StorageGRID

NetApp
December 03, 2025

Índice

Solucionar problemas de objetos e storage

Confirmar localizações de dados do objeto

Dependendo do problema, você pode querer "confirme 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.

Antes de começar

- 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 do "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 do "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. Se você quiser procurar uma versão específica do objeto, digite o ID da versão (opcional).

4. Selecione **Procurar**.

   O "resultados de pesquisa de metadados de objetos" aparece. Esta página lista os seguintes tipos de informações:

   - Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), 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",
```

Falhas no armazenamento de objetos (volume de storage)

O storage subjacente em um nó de storage é dividido em armazenamentos de objetos. 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
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

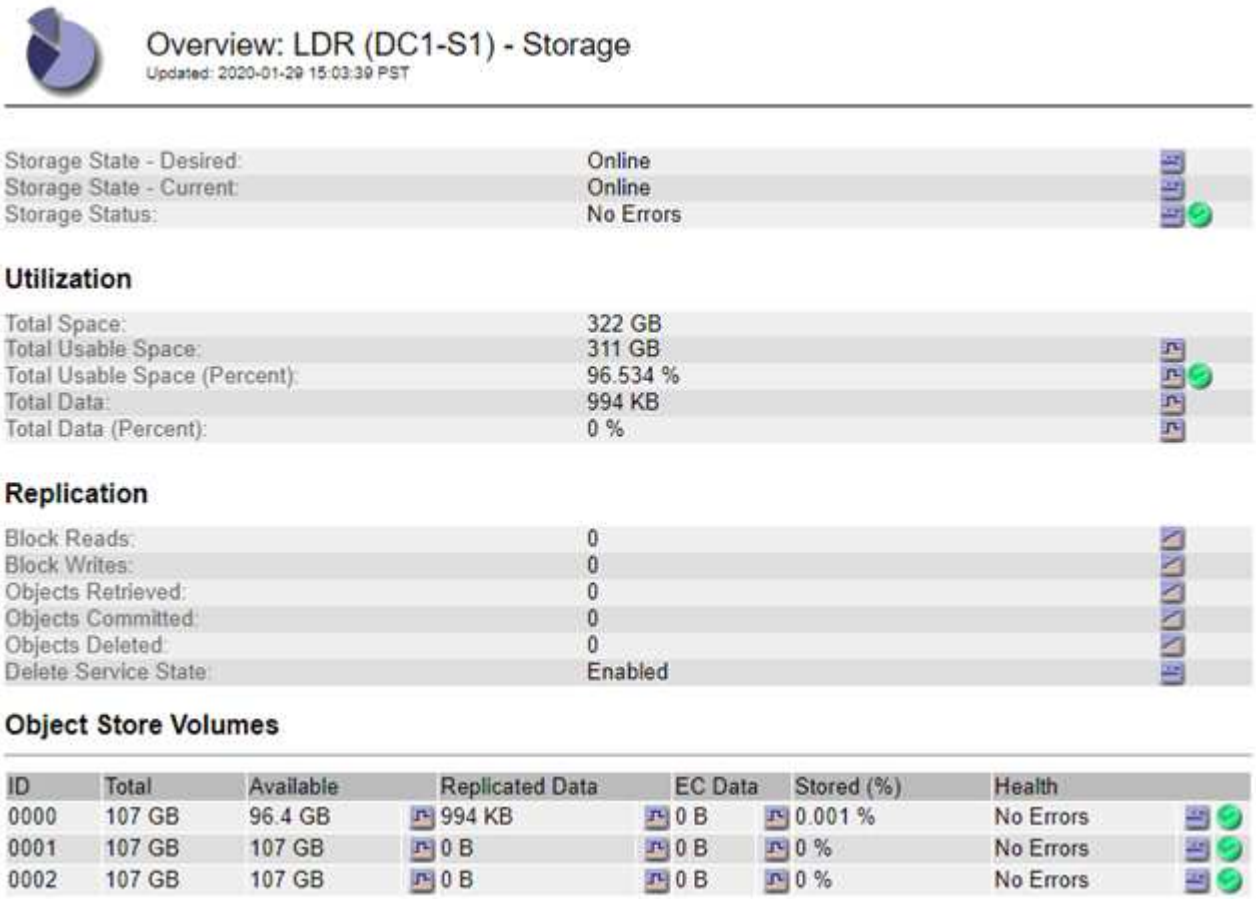
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	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
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	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 "Coloque o nó de storage em um estado somente leitura" para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto você se prepara para uma recuperação completa do servidor.

Verifique 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 de fundo e verificação de existência de objeto (anteriormente chamada de verificação de 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. Verificação de existência de objeto pode ser acionada por um usuário para verificar mais rapidamente a existência (embora não a correção) de objetos.

O que é a verificação em segundo plano?

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 as políticas ILM ativas. 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, 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 ele não pode 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** é acionado.

Altere 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.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

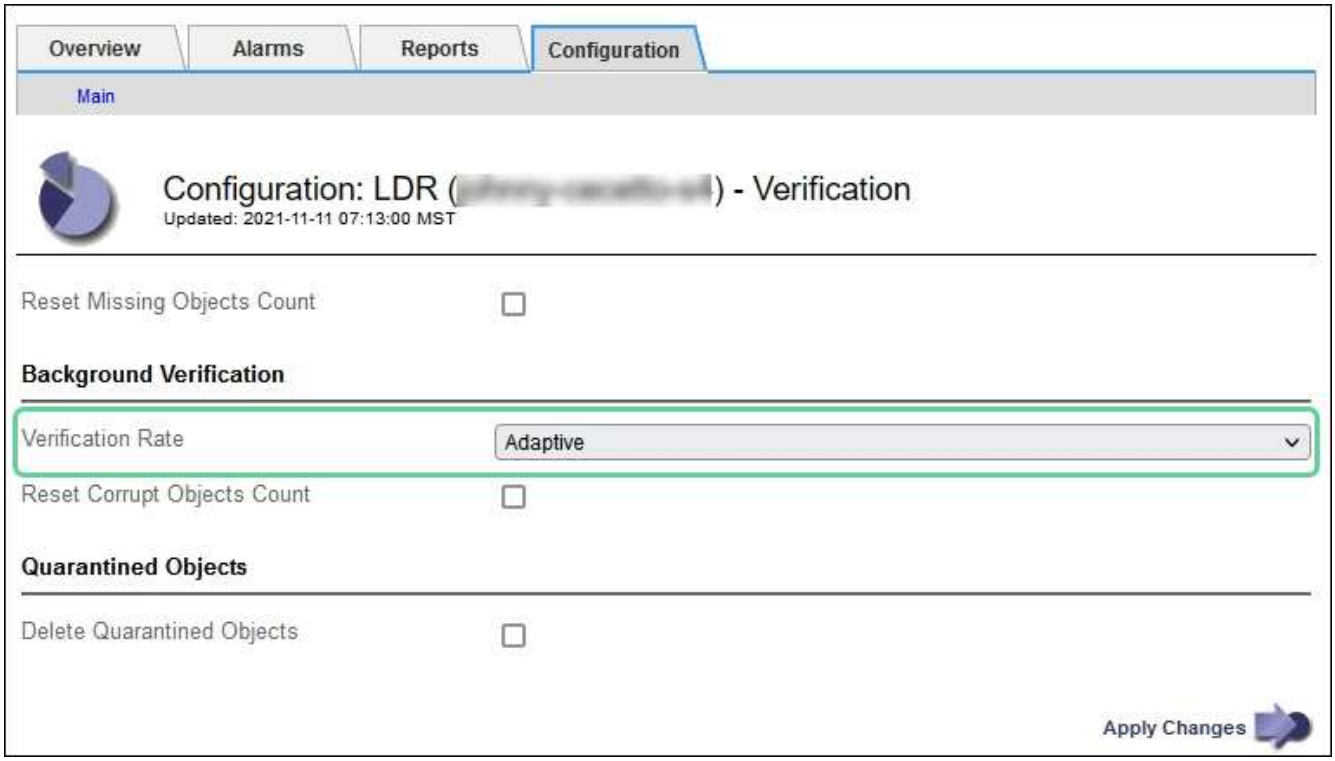
Você pode alterar a taxa de verificação para verificação em segundo plano em um nó de storage:

- 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** > **Verificação**.
3. Selecione **Configuração** > **Principal**.
4. Aceda a **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.

6. Clique em **aplicar alterações**.
7. 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 as políticas ativas de ILM.
- 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.

8. 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).

9. 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** > **Verificação** > **Configuração**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **aplicar alterações**.

10. 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.

    a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
    b. Selecione ***Storage Node*** > **LDR** > **Verificação** > **Configuração**.
    c. Selecione **Excluir objetos em quarentena**.
    d. Selecione **aplicar alterações**.

O que é verificação de existência de objeto?

A verificação de existência de objeto verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados por apagamento existem em um nó de storage. A verificação de existência do objeto não verifica os dados do objeto em si (a verificação em segundo plano faz isso); em vez disso, fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema de hardware recente poderia ter afetado a integridade dos dados.

Ao contrário da verificação em segundo plano, que ocorre automaticamente, você deve iniciar manualmente uma tarefa de verificação de existência de objeto.

A verificação de existência de objeto lê os metadados de cada objeto armazenado no StorageGRID e verifica a existência de cópias de objeto replicadas e fragmentos de objeto codificados por apagamento. Quaisquer dados em falta são tratados da seguinte forma:

- **Cópias replicadas**: Se uma cópia de dados de objetos replicados estiver ausente, o StorageGRID tentará substituir automaticamente a cópia de uma cópia armazenada 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 outra cópia está faltando. Uma nova cópia é gerada e colocada para satisfazer as políticas de ILM ativas do sistema. Esta nova cópia pode não ser colocada no mesmo local onde a cópia em falta foi armazenada.
- **Fragmentos 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 storage usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), o ILM tenta encontrar outra cópia do objeto, que ele pode usar para gerar um novo fragmento codificado de apagamento.

Executar verificação de existência de objeto

Você cria e executa um trabalho de verificação de existência de objeto de cada vez. Ao criar uma tarefa, você seleciona os nós de storage e os volumes que deseja verificar. Você também seleciona a consistência do trabalho.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Você garantiu que os nós de storage que deseja verificar estão online. Selecione **NÓS** para exibir a tabela de nós. Certifique-se de que nenhum ícone de alerta aparece ao lado do nome do nó para os nós que você deseja verificar.
- Você garantiu que os seguintes procedimentos estão **não** sendo executados nos nós que deseja verificar:
  - Expansão de grade para adicionar um nó de storage
  - Desativação do nó de storage
  - Recuperação de um volume de armazenamento com falha
  - Recuperação de um nó de armazenamento com uma unidade de sistema com falha
  - Rebalancear a EC
  - Clone de nó do dispositivo

A verificação existência de objeto não fornece informações úteis enquanto estes procedimentos estão em curso.

Sobre esta tarefa

Uma tarefa de verificação de existência de objeto pode levar dias ou semanas para ser concluída, dependendo do número de objetos na grade, dos nós e volumes de storage selecionados e da consistência selecionada. Você pode executar apenas uma tarefa de cada vez, mas pode selecionar vários nós e volumes de storage ao mesmo tempo.

Passos

1. Selecione **MAINTENANCE** > **Tasks** > **Object existence check**.
2. Selecione **criar trabalho**. O assistente criar uma tarefa de verificação de existência de objeto é exibido.

3. Selecione os nós que contêm os volumes que você deseja verificar. Para selecionar todos os nós on-line, marque a caixa de seleção **Nome do nó** no cabeçalho da coluna.

   Você pode pesquisar por nome do nó ou site.

   Não é possível selecionar nós que não estão conetados à grade.

4. Selecione **continuar**.
5. Selecione um ou mais volumes para cada nó na lista. Você pode pesquisar volumes usando o número do volume de armazenamento ou o nome do nó.

   Para selecionar todos os volumes para cada nó selecionado, marque a caixa de seleção **volume de armazenamento** no cabeçalho da coluna.

6. Selecione **continuar**.
7. Selecione a consistência do trabalho.

   A consistência determina quantas cópias dos metadados de objetos são usadas para a verificação de existência do objeto.

   - * Strong-site*: Duas cópias de metadados em um único site.
   - **Strong-global**: Duas cópias de metadados em cada local.
   - **Todos** (padrão): Todas as três cópias de metadados em cada site.

     Para obter mais informações sobre consistência, consulte as descrições no assistente.

8. Selecione **continuar**.
9. Reveja e verifique as suas seleções. Você pode selecionar **Previous** para ir para uma etapa anterior no assistente para atualizar suas seleções.

   Uma tarefa de verificação de existência de objeto é gerada e é executada até que uma das seguintes situações ocorra:

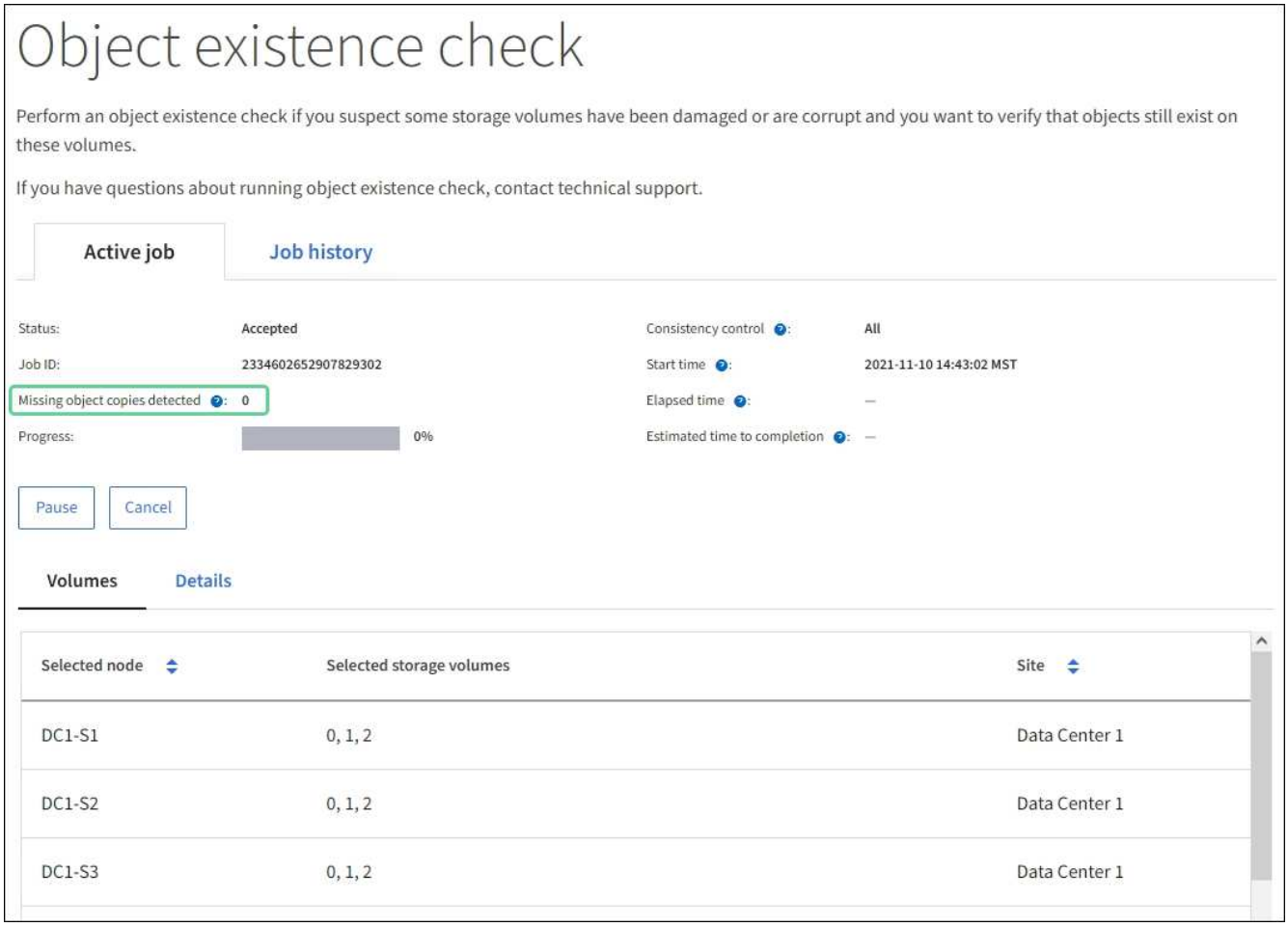
   - O trabalho é concluído.
   - Pausa ou cancelar o trabalho. Você pode retomar um trabalho em pausa, mas não pode retomar um trabalho cancelado.
   - O trabalho vai abaixo. O alerta **Object existence check has stalled** é acionado. Siga as ações corretivas especificadas para o alerta.
   - O trabalho falha. O alerta **Verificação de existência de objeto falhou** é acionado. Siga as ações corretivas especificadas para o alerta.
   - É apresentada uma mensagem "Service unavailable" (Serviço indisponível) ou "Internal Server error" (erro interno do servidor). Após um minuto, atualize a página para continuar a monitorizar o trabalho.

   > Conforme necessário, você pode navegar para longe da página de verificação existência de Objeto e retornar para continuar monitorando o trabalho.

10. À medida que a tarefa é executada, exiba a guia **trabalho ativo** e observe o valor de cópias de objetos ausentes detetadas.

    Esse valor representa o número total de cópias ausentes de objetos replicados e objetos codificados por apagamento com um ou mais fragmentos ausentes.

Se o número de cópias de objetos ausentes detetadas for maior que 100, pode haver um problema com o armazenamento do nó de armazenamento.



11. Após a conclusão do trabalho, execute quaisquer ações adicionais necessárias:
    - Se as cópias de objeto em falta detetadas forem zero, não foram encontrados problemas. Nenhuma ação é necessária.
    - Se as cópias de objetos em falta detetadas forem maiores que zero e o alerta **objetos perdidos** não tiver sido acionado, todas as cópias em falta foram reparadas pelo sistema. Verifique se quaisquer problemas de hardware foram corrigidos para evitar danos futuros às cópias de objetos.
    - Se as cópias de objetos em falta detetadas forem maiores que zero e o alerta **objetos perdidos** tiver sido acionado, a integridade dos dados poderá ser afetada. Entre em Contato com o suporte técnico.
    - Você pode investigar cópias de objetos perdidos usando grep para extrair as mensagens de auditoria LLST: `grep LLST audit_file_name`.

      Este procedimento é semelhante ao de "investigando objetos perdidos", embora para cópias de objetos que você pesquise em `LLST` vez `OLST` de .

12. Se você selecionou a consistência forte ou forte-global para a tarefa, aguarde aproximadamente três semanas pela consistência dos metadados e execute novamente a tarefa nos mesmos volumes novamente.

    Quando o StorageGRID tiver tido tempo para alcançar a consistência de metadados para os nós e volumes incluídos na tarefa, a execução novamente da tarefa pode limpar cópias de objetos ausentes relatadas erroneamente ou fazer com que cópias de objetos adicionais sejam verificadas se elas foram

perdidas.

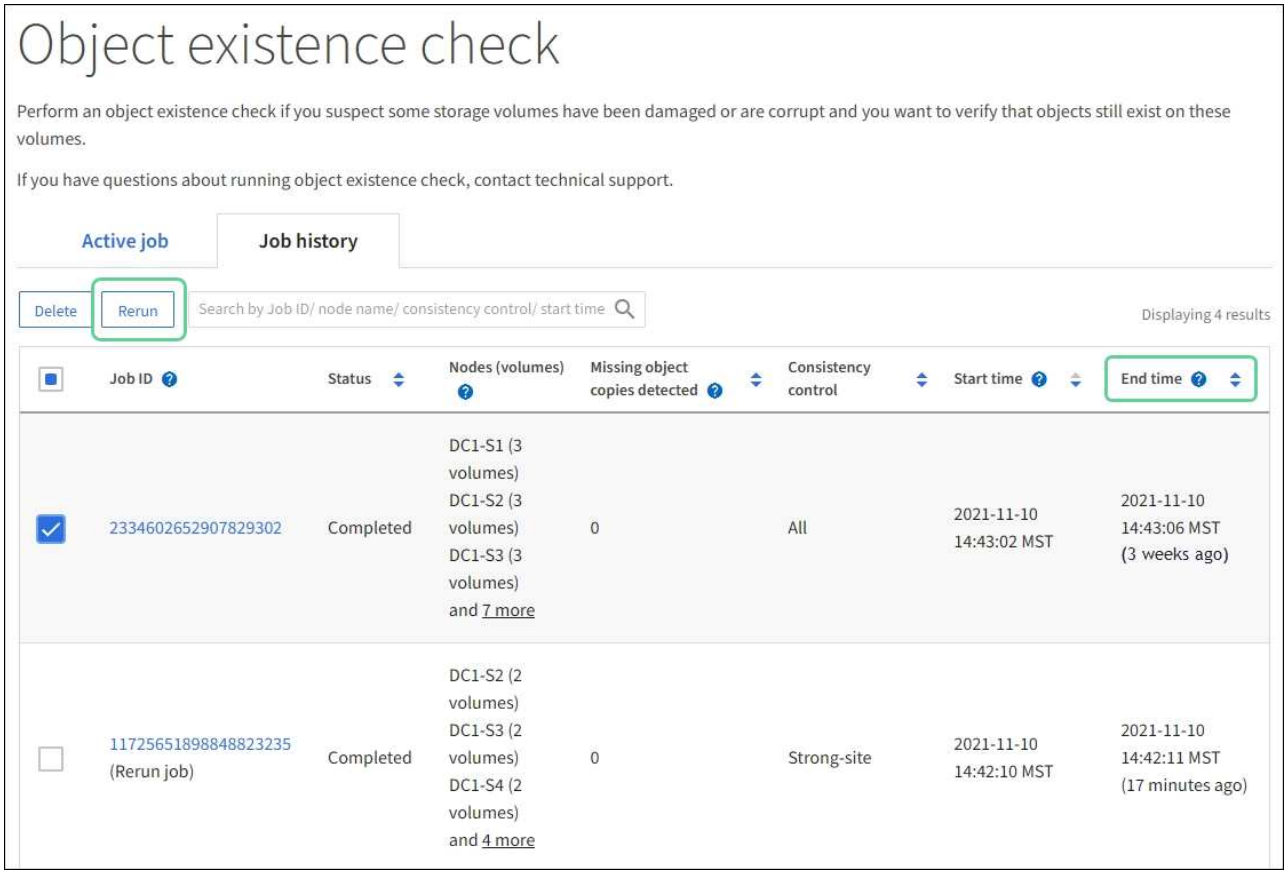
a. Selecione **MAINTENANCE** > **Object existence check** > **Job history**.

b. Determine quais trabalhos estão prontos para serem executados novamente:

   i. Olhe para a coluna **hora de fim** para determinar quais trabalhos foram executados há mais de três semanas.

   ii. Para esses trabalhos, examine a coluna de controle de consistência para sites fortes ou globais.

c. Selecione a caixa de verificação para cada trabalho que pretende executar novamente e, em seguida, selecione **Reexecutar**.



d. No assistente de reexecução de trabalhos, reveja os nós e volumes selecionados e a consistência.

e. Quando estiver pronto para executar novamente os trabalhos, selecione **Reexecutar**.

É apresentado o separador trabalho ativo. Todos os trabalhos selecionados são reexecutados como um trabalho com consistência de um local forte. Um campo **trabalhos relacionados** na seção Detalhes lista os IDs dos trabalhos originais.

Depois de terminar

Se ainda tiver preocupações sobre a integridade dos dados, aceda a **SUPPORT** > **Tools** > **Grid topoly** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** 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.

Resolução de problemas S3 COLOQUE o alerta tamanho do objeto demasiado grande

O alerta S3 PUT Object Size too large (tamanho do objeto de COLOCAÇÃO muito grande) é acionado se um locatário tentar uma operação PutObject não multiparte que exceda o limite de tamanho S3 de 5 GiB.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Determine quais locatários usam objetos maiores que 5 GiB, para que você possa notificá-los.

Passos

1. Aceda a **CONFIGURATION** > **Monitoring** > **Audit and syslog Server**.
2. Se as gravações do cliente forem normais, acesse o log de auditoria:

   a. Introduza `ssh admin@primary_Admin_Node_IP`

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

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

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

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

   e. Mude para o diretório onde os logs de auditoria estão localizados.

   O diretório de log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	`/var/local/log/localaudit.log`
Nós de administração/nós locais	• Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

   Dependendo das definições de destino da auditoria, introduza: `cd /var/local/log` Ou `/var/local/audit/export/`

   Para saber mais, "Selecione destinos de informações de auditoria"consulte .

   f. Identifique quais locatários estão usando objetos maiores que 5 GiB.

i. Introduza `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

ii. Para cada mensagem de auditoria nos resultados, observe `S3AI` o campo para determinar o ID da conta do locatário. Use os outros campos da mensagem para determinar qual endereço IP foi usado pelo cliente, pelo bucket e pelo objeto:

Código	Descrição
SAIP	IP de origem
S3AI	ID do inquilino
S3BK	Balde
S3KY	Objeto
CSIZ	Tamanho (bytes)

Exemplo de resultados de log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CSTR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:identity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][SBAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Se as gravações do cliente não forem normais, use o ID do locatário do alerta para identificar o locatário:

a. Aceda a **SUPPORT** > **Tools** > **Logs**. Colete logs de aplicativos para o nó de armazenamento no alerta. Especifique 15 minutos antes e depois do alerta.

b. Extraia o arquivo e vá `bycast.log` para :

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

c. PESQUISE o log `method=PUT` e identifique o cliente no `clientIP` campo.

Exemplo bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informe aos locatários que o tamanho máximo do PutObject é de 5 GiB e para usar uploads de várias partes para objetos maiores que 5 GiB.
5. Ignore o alerta por uma semana se o aplicativo tiver sido alterado.

Solucionar problemas de dados de objetos perdidos e ausentes

Solucionar problemas de dados de objetos perdidos e ausentes: Visão geral

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** é acionado, da seguinte forma:

- Para cópias replicadas, se outra cópia não puder ser recuperada, o objeto será considerado perdido e o alerta será acionado.
- Para cópias codificadas por apagamento, se uma cópia não puder ser recuperada do local esperado, o atributo cópias corrompidas detetadas (ECOR) será incrementado por um antes de uma tentativa ser feita para recuperar uma cópia de outro local. Se nenhuma outra cópia for encontrada, o alerta é acionado.

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. "Investigue objetos perdidos"Consulte .

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. "Repor contagens de objetos perdidas e em falta"Consulte .

Investigue objetos perdidos

Quando o alerta **Objects Lost** é acionado, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em Contato com o suporte técnico.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

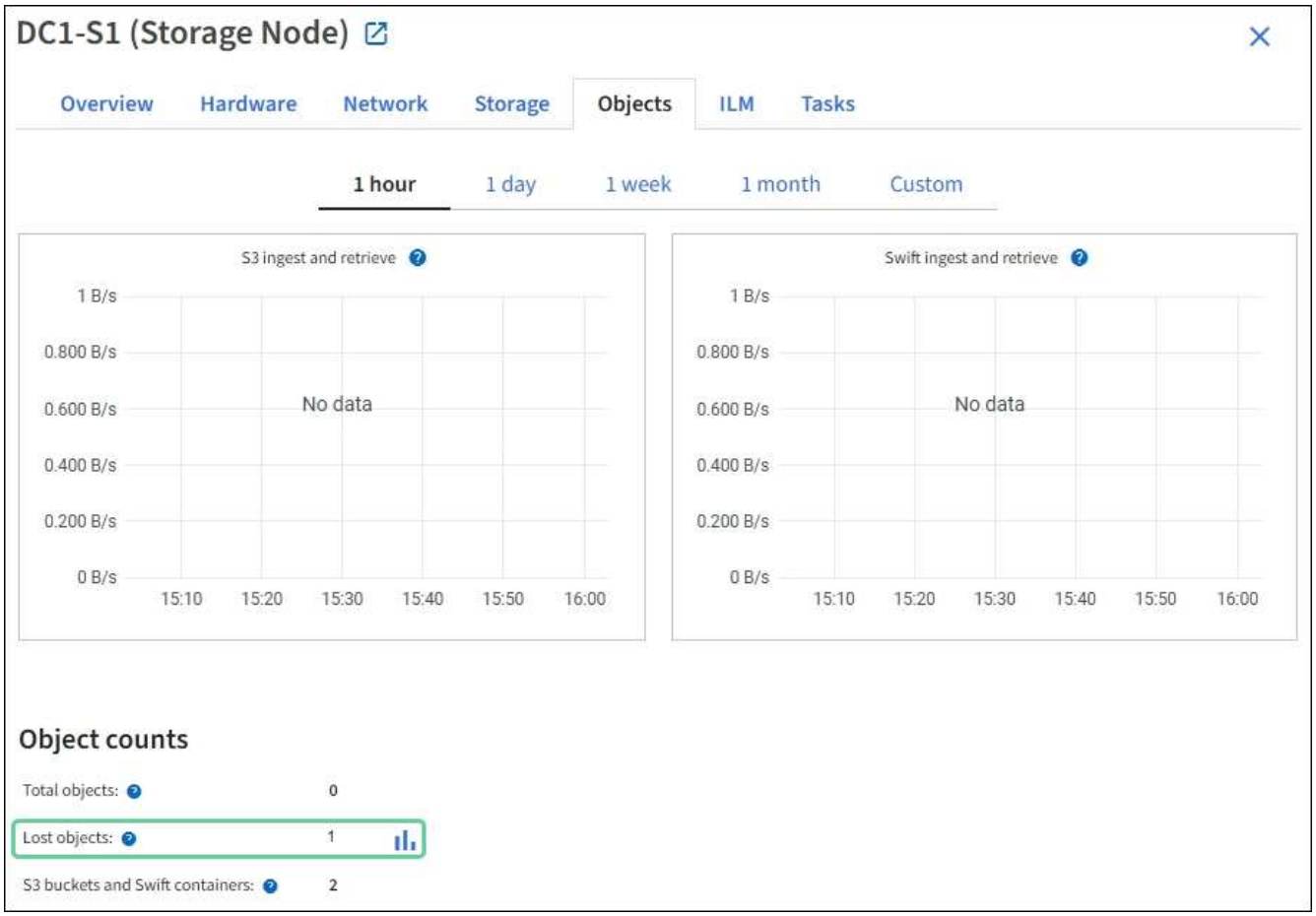
O alerta **objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

Investigue 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.

Passos

1. Selecione **NODES**.
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**:
   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.

O diretório de log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	`/var/local/log/localaudit.log`
Nós de administração/nós locais	• Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

Dependendo das definições de destino da auditoria, introduza: `cd /var/local/log` Ou `/var/local/audit/export/`

Para saber mais, "Selecione destinos de informações de auditoria"consulte .

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. Use SSH para fazer login em qualquer nó de armazenamento. Em seguida, aceda à consola LDR introduzindo "telnet 0 1402".

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, você pode redefinir a contagem de **objetos perdidos** para limpar o alerta. A falta de um objeto indica que o objeto foi intencionalmente excluído.
Localizações > 0	Se houver locais listados na saída, o alerta **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 "procurar objetos potencialmente perdidos" explica como usar o ID do nó para encontrar o nó de armazenamento correto.) Se os objetos existirem, você pode redefinir a contagem de **objetos perdidos** para limpar o alerta.
Localização: 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar "procure e restaure o objeto" para si mesmo, ou você pode entrar em Contato com o suporte técnico. O suporte técnico pode pedir-lhe para determinar se existe um procedimento de recuperação de armazenamento em curso. Consulte as informações sobre "Restaurando dados de objetos usando o Grid Manager" e "restaurar dados de objeto para um volume de armazenamento".

Procure e restaure 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.

Antes de começar

- Você tem o UUID de qualquer objeto perdido, conforme identificado em "Investigue objetos perdidos".
- Você tem o `Passwords.txt` arquivo.

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.

      O diretório de log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	`/var/local/log/localaudit.log`
Nós de administração/nós locais	• Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

      Dependendo das definições de destino da auditoria, introduza: `cd /var/local/log` Ou `/var/local/audit/export/`

      Para saber mais, "Selecione destinos de informações de auditoria"consulte .

   c. Use grep para extrair o "auditar mensagens associadas ao objeto potencialmente perdido" e enviá-los 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 >
/var/local/tmp/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 /var/local/tmp/messages_about_lost_objects.txt
```

Uma mensagem de auditoria LLST se parece com esta 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):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
86871083190743409]]
```

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.

a. Localize o nó de armazenamento associado a este ID de nó LDR. No Gerenciador de Grade, selecione **support** > **Tools** > **Grid topology**. Em seguida, selecione ***Data Center*** > ***Storage Node*** > **LDR**.

O ID do nó para o serviço LDR está na tabela informações do nó. Reveja as informações de cada nó de armazenamento até encontrar o que hospeda este LDR.

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'
```

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 próxima etapa. Você pode tentar restaurar o objeto encontrado de volta para o StorageGRID.

3. 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. Use SSH para fazer login em qualquer nó de armazenamento. Em seguida, aceda à consola LDR introduzindo "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 as políticas ILM ativas, que fazem cópias adicionais conforme especificado em cada política.

      > 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 seguinte.

4. 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`

5. 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. subetapa 1. bConsulte a .

   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 >
      /var/local/tmp/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 /var/local/tmp/messages_about_restored_object.txt
      ```

      Uma mensagem de auditoria ORLM se parece com esta 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.

6. "Redefina as contagens de objetos perdidas e ausentes" No Gerenciador de Grade.

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.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

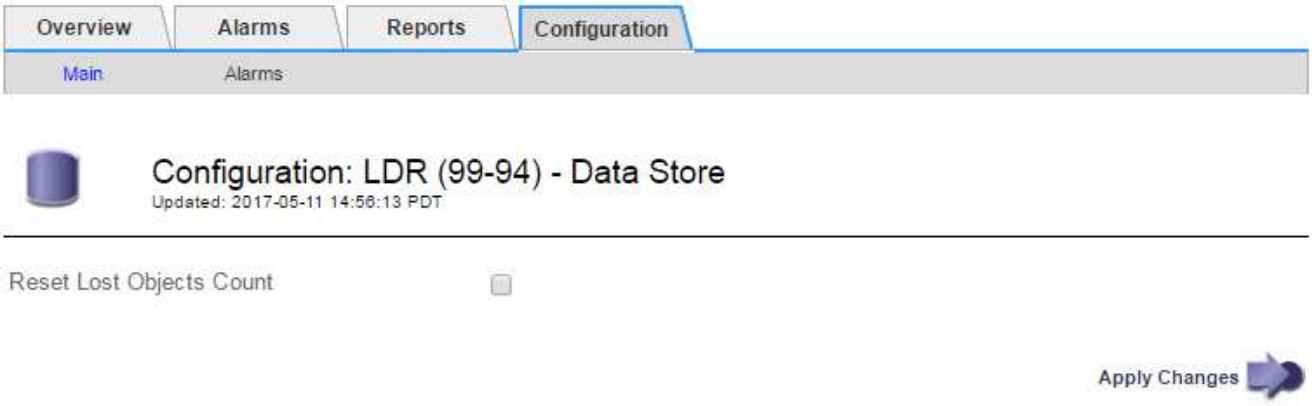
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

- **SUPORTE** > **Ferramentas** > **topologia de grelha** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Overview** > **Main**
- **SUPORTE** > **Ferramentas** > **topologia de grelha** > ***Site*** > ***Storage Node*** > **DDS** > **Data Store** > **Visão geral** > **Main**

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** > **armazenamento de dados** > **Configuração** 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** > **Codificação de apagamento** > **Configuração**.

   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).

Solucionar 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.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

O alerta **armazenamento de dados de objeto baixo** é acionado quando a quantidade total de dados de objeto replicados e codificados por apagamento 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 de dados de objetos replicados e codificados por apagamento 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.

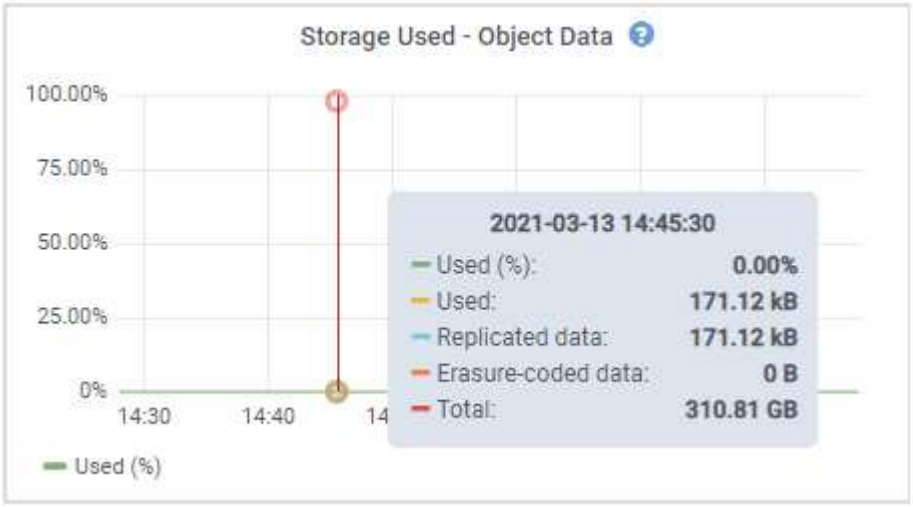
   Selecione o alerta e não o cabeçalho de um grupo de alertas.

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. Posicione o cursor sobre o gráfico 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, "adicionar capacidade de armazenamento" para a sua grade.

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

   Para obter mais informações, "Gerencie nós de storage completos"consulte .

Informações relacionadas

"Resolução de problemas do alarme de estado de armazenamento (SSTS) (legado)"

Solucionar problemas de alertas de substituição de marca d'água somente leitura baixa

Se você usar valores personalizados para marcas d'água de volume de armazenamento, talvez seja necessário resolver o alerta **baixa substituição de marca d'água somente leitura**. Se possível, você deve atualizar seu sistema para começar a usar os valores otimizados.

Nas versões anteriores, as três "marcas de água do volume de armazenamento" eram configurações globais e número 8212; os mesmos valores aplicados a cada volume de armazenamento em cada nó de armazenamento. A partir do StorageGRID 11,6, o software pode otimizar essas marcas d'água para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Quando você atualiza para o StorageGRID 11,6 ou superior, marcas de água otimizadas somente leitura e leitura-gravação são aplicadas automaticamente a todos os volumes de armazenamento, a menos que uma das seguintes opções seja verdadeira:

- Seu sistema está próximo da capacidade e não poderá aceitar novos dados se forem aplicadas marcas de água otimizadas. Neste caso, o StorageGRID não alterará as configurações de marca d'água.
- Você definiu anteriormente qualquer uma das marcas d'água do volume de armazenamento para um valor personalizado. O StorageGRID não substituirá as configurações personalizadas de marca d'água com valores otimizados. No entanto, o StorageGRID pode acionar o alerta de substituição de marca d'água **baixa somente leitura** se o valor personalizado para a marca d'água de volume de armazenamento Soft somente leitura for muito pequeno.

Entenda o alerta

Se você usar valores personalizados para marcas d'água de volume de armazenamento, o alerta **Sobreposição de marca d'água somente leitura baixa** pode ser acionado para um ou mais nós de armazenamento.

Cada instância do alerta indica que o valor personalizado do **Storage volume Soft Read-Only Watermark** é menor do que o valor otimizado mínimo para esse Storage Node. Se você continuar a usar a configuração personalizada, o nó de armazenamento pode ser executado criticamente baixo no espaço antes que ele possa fazer a transição com segurança para o estado somente leitura. Alguns volumes de armazenamento podem ficar inacessíveis (desmontados automaticamente) quando o nó atinge a capacidade.

Por exemplo, suponha que você tenha definido anteriormente o **Storage volume Soft Read-Only Watermark** para 5 GB. Agora suponha que o StorageGRID calculou os seguintes valores otimizados para os quatro volumes de armazenamento no nó de armazenamento A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB
Volume 3	15 GB

O alerta **Low read-only watermark override** é acionado para o nó de armazenamento A porque sua marca d'água personalizada (5 GB) é menor do que o valor otimizado mínimo para todos os volumes nesse nó (11 GB). Se você continuar usando a configuração personalizada, o nó pode ser executado criticamente baixo no espaço antes que ele possa fazer a transição com segurança para o estado somente leitura.

Resolva o alerta

Siga estes passos se um ou mais alertas de substituição de marca d'água somente leitura baixa* tiverem sido acionados. Você também pode usar essas instruções se você usar configurações personalizadas de marca d'água atualmente e quiser começar a usar configurações otimizadas, mesmo que nenhum alerta tenha sido acionado.

Antes de começar

- Concluiu a atualização para o StorageGRID 11,6 ou superior.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

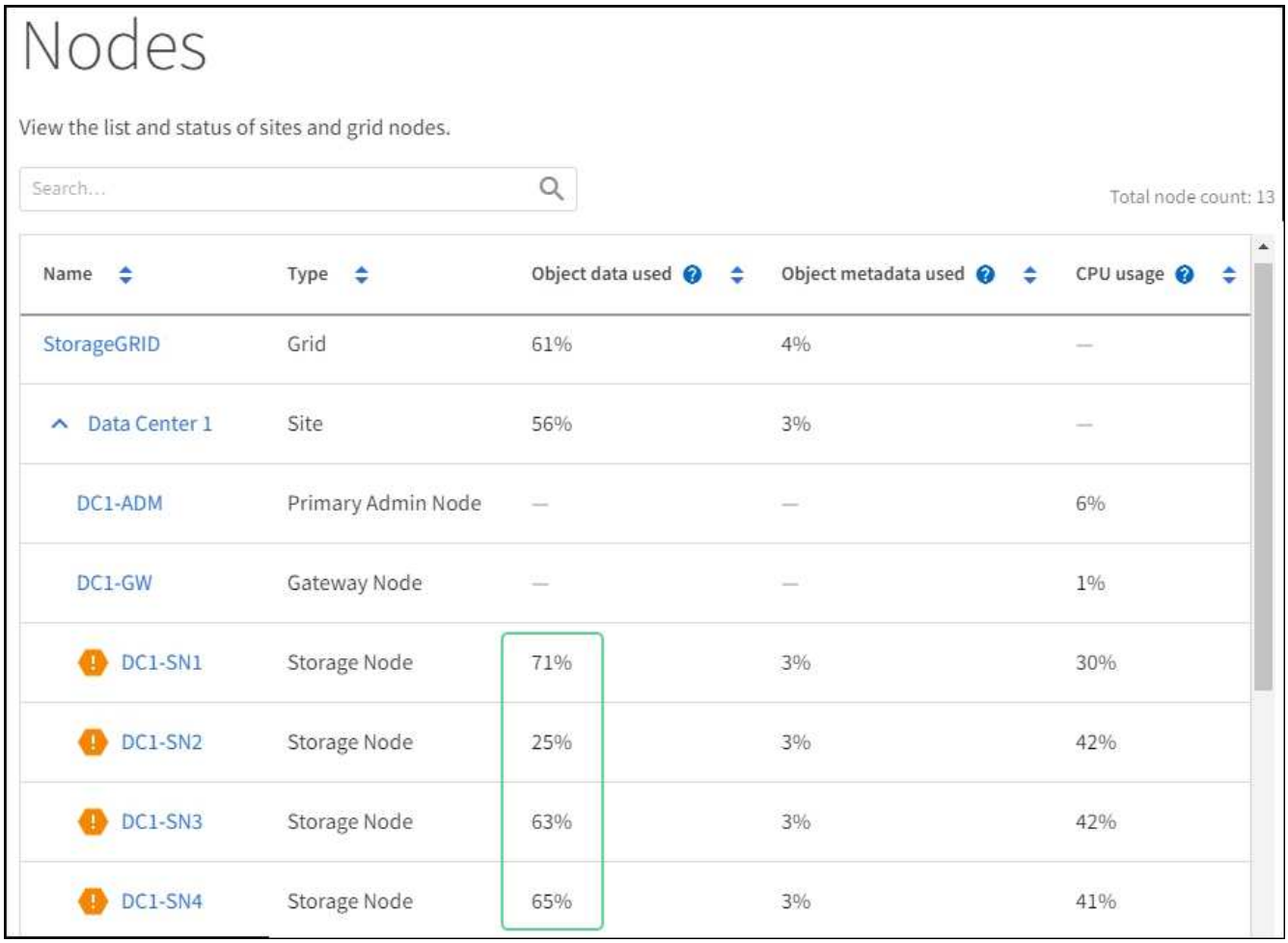
Sobre esta tarefa

Você pode resolver o alerta * baixa substituição de marca d'água somente leitura * atualizando as configurações personalizadas de marca d'água para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem próximos do cheio ou se você tiver requisitos especiais de ILM, primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados de objeto para toda a grade

Passos

1. Selecione **NODES**.
2. Para cada local na grade, expanda a lista de nós.
3. Revise os valores de porcentagem mostrados na coluna **dados de objeto usados** para cada nó de armazenamento em cada local.



4. Siga o passo apropriado:
   a. Se nenhum dos nós de armazenamento estiver próximo da totalidade (por exemplo, todos os valores **dados de objeto usados** forem inferiores a 80%), você poderá começar a usar as configurações de substituição. Vá para Use marcas de água otimizadas.
   b. Se as regras do ILM usarem comportamento de ingestão rigoroso ou se os pools de armazenamento específicos estiverem próximos de cheio, execute as etapas em Ver marcas de água de armazenamento otimizadas e Determine se você pode usar marcas de água otimizadas.

Ver marcas de água de armazenamento otimizadas

O StorageGRID usa duas métricas Prometheus para mostrar os valores otimizados que calculou para a marca d'água **volume de armazenamento Soft Read-Only**. Você pode visualizar os valores otimizados mínimo e máximo para cada nó de storage em sua grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **Metrics**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário Prometheus.
3. Para ver a marca d'água mínima de leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor mínimo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para o **Storage volume Soft Read-Only Watermark**, o alerta **Low read-only Watermark** (Sobreposição de marca d'água somente leitura baixa) será acionado para o Storage Node.

4. Para ver a marca d'água somente leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor máximo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento.

5. Observe o valor otimizado máximo para cada nó de armazenamento.

determine se você pode usar marcas de água otimizadas

Passos

1. Selecione **NODES**.
2. Repita estas etapas para cada nó de armazenamento online:
   a. Selecione ***Storage Node*** > **Storage**.
   b. Role para baixo até a tabela Object Stores.
   c. Compare o valor **disponível** para cada armazenamento de objetos (volume) com a marca d'água máxima otimizada que você anotou para esse nó de armazenamento.
3. Se pelo menos um volume em cada nó de armazenamento online tiver mais espaço disponível do que a marca d'água máxima otimizada para esse nó, vá para começar a usar as marcas d'Use marcas de água otimizadaságua otimizadas.

   Caso contrário, expanda a grade o mais rápido possível. "adicione volumes de armazenamento"Para um nó existente ou "Adicionar novos nós de storage". Em seguida, aceda a Use marcas de água otimizadas para atualizar as definições da marca de água.

4. Se você precisar continuar usando valores personalizados para as marcas d'água do volume de armazenamento, "silêncio" ou "desativar" o alerta **Sobreposição de marca d'água somente leitura baixa**.

Os mesmos valores de marca d'água personalizados são aplicados a cada volume de armazenamento em cada nó de armazenamento. O uso de valores menores que os recomendados para marcas d'água de volume de armazenamento pode fazer com que alguns volumes de armazenamento fiquem inacessíveis (desmontados automaticamente) quando o nó atinge a capacidade.

[[marcas de água otimizadas para uso]]Use marcas de água otimizadas

Passos

1. Aceda a **SUPPORT** > **Other** > **Storage watermarks**.
2. Marque a caixa de seleção **usar valores otimizados**.
3. Selecione **Guardar**.

As configurações de marca d'água de volume de armazenamento otimizadas estão agora em vigor para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Solucione o problema do alarme de Status 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.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

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 (**CONFIGURATION** > **System** > **Storage options**).

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

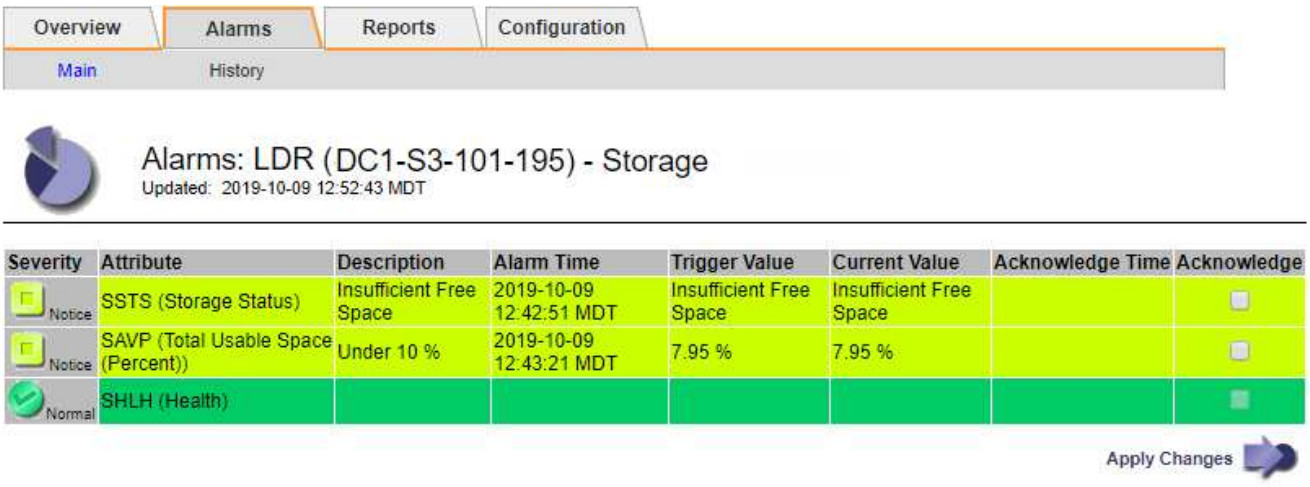
Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. O alarme SSTS é acionado se menos de 10 GB de espaço utilizável permanecer em cada volume de armazenamento no nó de armazenamento. Se algum dos volumes tiver 10 GB ou mais de 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 **SUPPORT** > **Alarmes (legacy)** > **Current Alarmes**.
2. Na coluna Serviço, selecione o data center, o nó e o serviço associados ao alarme SSTS.

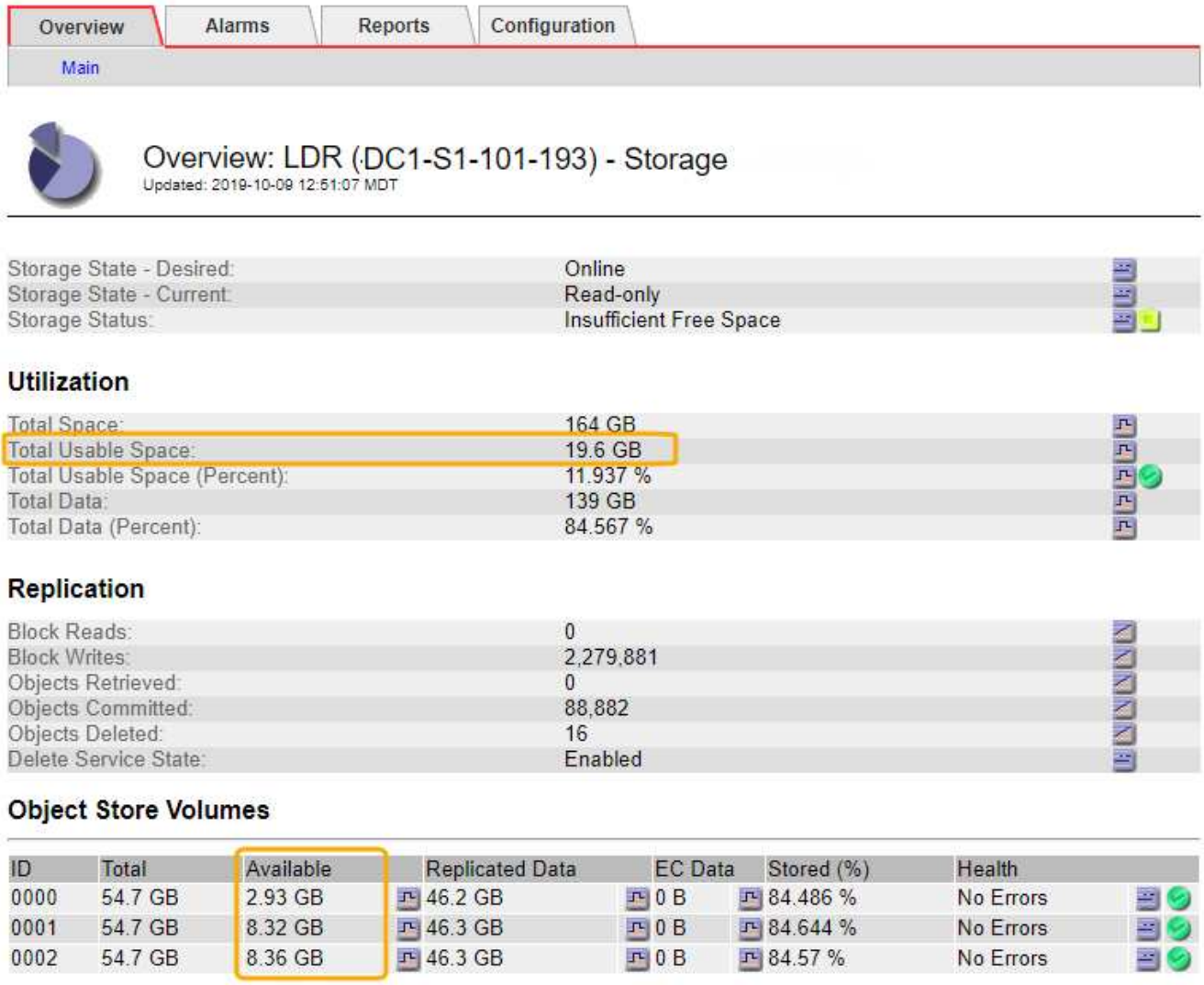
   É apresentada a página Grid Topology (topologia de grelha). A guia Alarmes mostra os alarmes ativos para o nó e serviço selecionados.



   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.

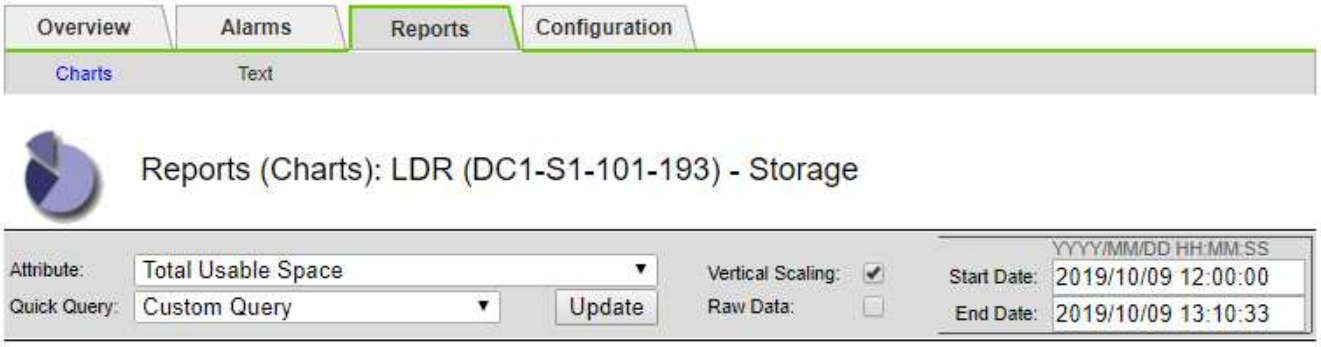
3. Para determinar quanto espaço utilizável está realmente disponível, selecione **LDR** > **Storage** > **Overview** e encontre o atributo espaço utilizável total (STAS).

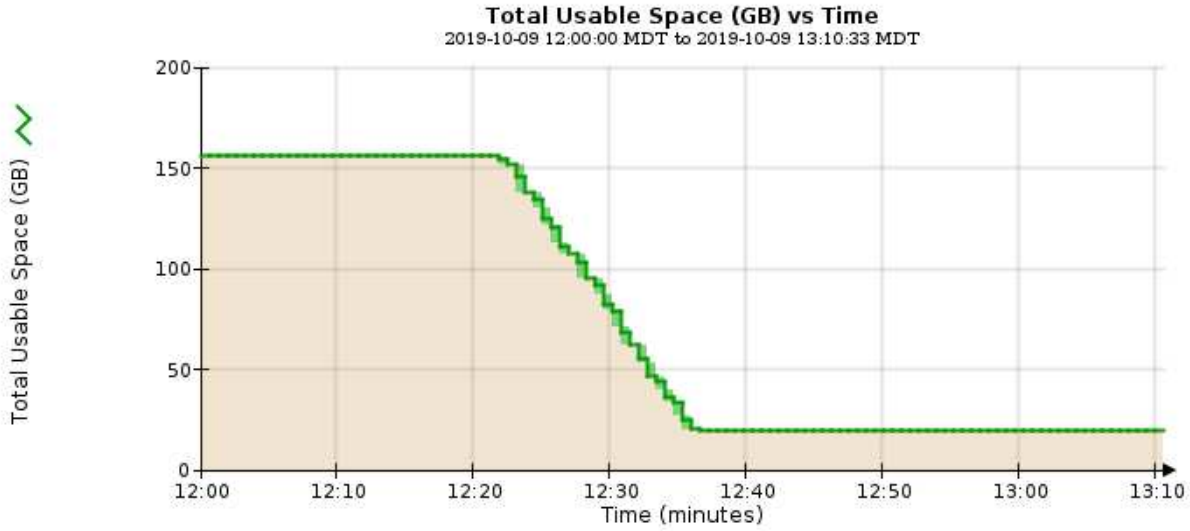


Neste exemplo, apenas 19,6 GB dos 164 GB de espaço neste nó de armazenamento permanecem disponíveis. Observe que o valor total é a soma dos valores **disponíveis** para os três volumes de armazenamento de objetos. O alarme SSTS foi acionado porque cada um dos três volumes de armazenamento tinha menos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

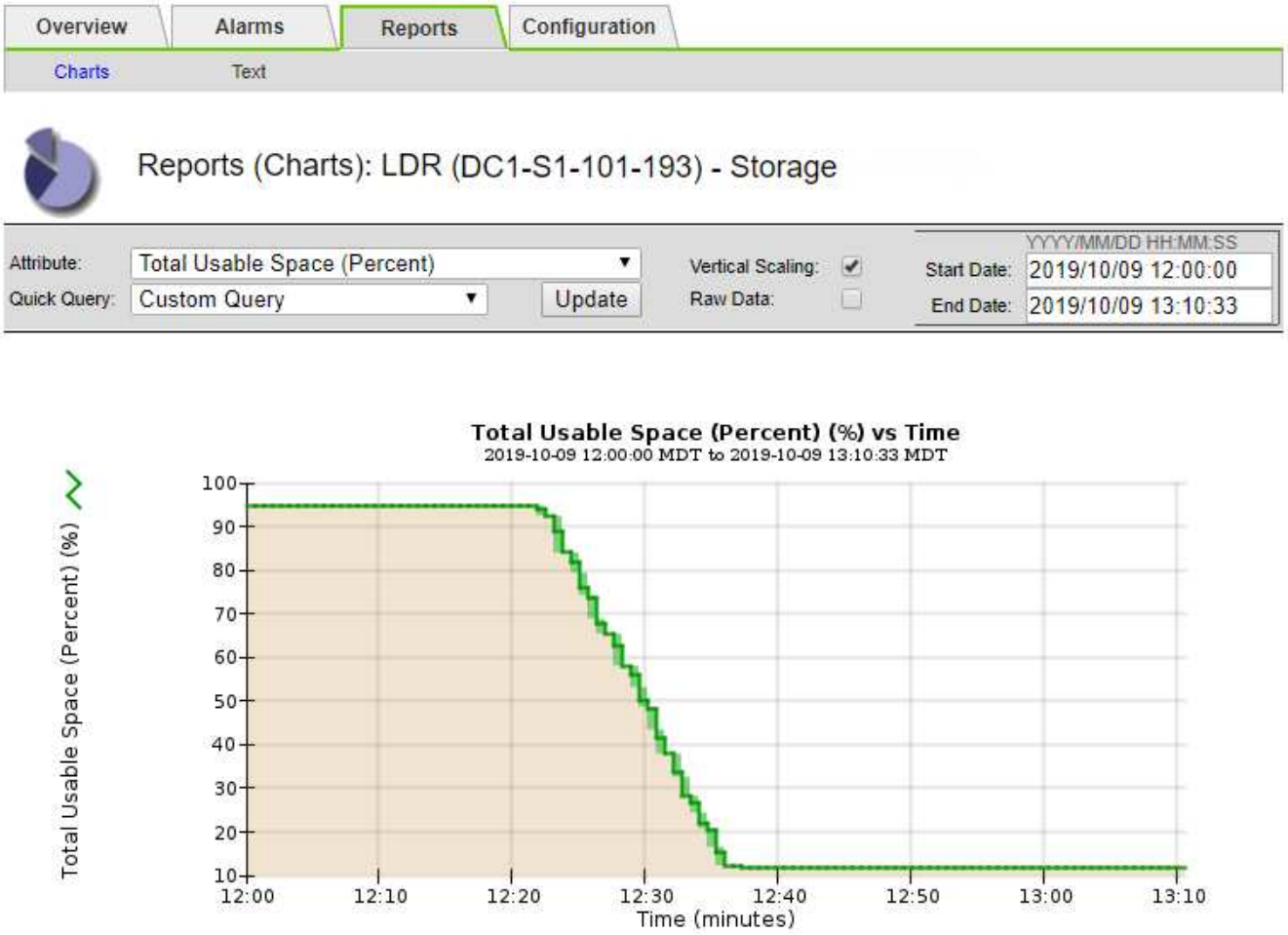
   Neste exemplo, o espaço utilizável total caiu de cerca de 155 GB em 12:00 para 20 GB em 12:35, o que corresponde ao momento em que o alarme SSTS foi acionado.





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, "adicionar capacidade de armazenamento".

   Consulte também "Gerencie nós de storage completos".

Solucionar 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 de 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.

As mensagens de evento também são listadas no `/var/local/log/bycast-err.log` arquivo de log. Consulte "Referência de ficheiros de registo".

Para obter informações adicionais, consulte o "Solucionar problemas de serviços de plataforma". Talvez seja necessário "Acesse o locatário do Gerenciador do Locatário"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. Selecione **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 sobre direitos autorais

Informações sobre marcas comerciais