Solucionar problemas do sistema StorageGRID

StorageGRID software

NetApp
December 03, 2025

Índice

Solucionar problemas do sistema StorageGRID

Solucionar problemas de um sistema StorageGRID

Se você encontrar um problema ao usar um sistema StorageGRID , consulte as dicas e diretrizes nesta seção para obter ajuda para determinar e resolver o problema.

Muitas vezes, você pode resolver problemas sozinho; no entanto, pode ser necessário encaminhar alguns problemas ao suporte técnico.

Defina o problema

O primeiro passo para resolver um problema é defini-lo claramente.

Esta tabela fornece exemplos dos tipos de informações que você pode coletar para definir um problema:

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não fazendo? Quais são os sintomas?	Os aplicativos clientes estão relatando que objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez por volta das 14h50 do dia 8 de janeiro de 2020.
Como você percebeu o problema pela primeira vez?	Notificado pelo aplicativo do cliente. Também recebi notificações de alerta por e-mail.
O problema acontece constantemente ou apenas às vezes?	O problema continua.
Se o problema acontece regularmente, quais etapas fazem com que ele ocorra?	O problema acontece sempre que um cliente tenta ingerir um objeto.
Se o problema acontece intermitentemente, quando ele ocorre? Registre os horários de cada incidente que você tiver conhecimento.	O problema não é intermitente.
Você já viu esse problema antes? Com que frequência você teve esse problema no passado?	Esta é a primeira vez que vejo esse problema.

Avaliar o risco e o impacto no sistema

Depois de definir o problema, avalie seu risco e impacto no sistema StorageGRID . Por exemplo, a presença de alertas críticos não significa necessariamente que o sistema não esteja prestando serviços essenciais.

Esta tabela resume o impacto que o problema de exemplo está tendo nas operações do sistema:

Pergunta	Exemplo de resposta
O sistema StorageGRID pode ingerir conteúdo?	Não.
Os aplicativos clientes podem recuperar conteúdo?	Alguns objetos podem ser recuperados e outros não.
Os dados estão em risco?	Não.
A capacidade de conduzir negócios é severamente afetada?	Sim, porque os aplicativos clientes não podem armazenar objetos no sistema StorageGRID e os dados não podem ser recuperados de forma consistente.

Coletar dados

Depois de definir o problema e avaliar seu risco e impacto, colete dados para análise. O tipo de dado mais útil para coletar depende da natureza do problema.

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Criar cronograma de mudanças recentes	Alterações no seu sistema StorageGRID , sua configuração ou seu ambiente podem causar novos comportamentos.	• Crie uma linha do tempo das mudanças recentes
Alertas de revisão	Os alertas podem ajudar você a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso. Revise a lista de alertas atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Revise os alertas acionados no passado para obter insights adicionais.	• "Ver alertas atuais e resolvidos"
Monitorar eventos	Eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas surgiram pela primeira vez e podem ajudar você a entender a rapidez com que as coisas estão mudando.	• "Use tabelas e gráficos" • "Usar relatórios de texto"

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Estabelecer linhas de base	Colete informações sobre os níveis normais de vários valores operacionais. Esses valores de base e desvios dessas linhas de base podem fornecer pistas valiosas.	• Estabelecer linhas de base
Realizar testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com aqueles vistos ao usar o aplicativo cliente.	• "Monitore o desempenho de PUT e GET"
Revisar mensagens de auditoria	Revise as mensagens de auditoria para acompanhar as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Revisar mensagens de auditoria"
Verifique a localização dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de armazenamento.	• "Monitorar operações de verificação de objetos" • "Confirmar a localização dos dados do objeto" • "Verificar integridade do objeto"
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	• "Coletar arquivos de log e dados do sistema" • "Acionar manualmente um pacote AutoSupport" • "Revisar métricas de suporte"

Criar uma linha do tempo das mudanças recentes

Quando ocorre um problema, você deve considerar o que mudou recentemente e quando essas mudanças ocorreram.

- Alterações no seu sistema StorageGRID , sua configuração ou seu ambiente podem causar novos comportamentos.
- Um cronograma de mudanças pode ajudar você a identificar quais mudanças podem ser responsáveis por um problema e como cada mudança pode ter afetado seu desenvolvimento.

Crie uma tabela de alterações recentes no seu sistema que inclua informações sobre quando cada alteração ocorreu e quaisquer detalhes relevantes sobre a alteração, como informações sobre o que mais estava acontecendo enquanto a alteração estava em andamento:

Tempo de mudança	Tipo de mudança	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização do software foi concluída? • Você interrompeu o processo?	O que aconteceu? O que você fez?	Documente quaisquer detalhes relevantes sobre a mudança. Por exemplo: • Detalhes das alterações na rede. • Qual hotfix foi instalado. • Como as cargas de trabalho dos clientes mudaram. Não deixe de anotar se mais de uma alteração estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi instalado, expandido ou recuperado recentemente?
- O sistema foi atualizado recentemente? Foi aplicado algum hotfix?
- Algum hardware foi reparado ou trocado recentemente?
- A política do ILM foi atualizada?
- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento mudou?
- Você alterou os balanceadores de carga ou adicionou ou removeu um grupo de alta disponibilidade de nós de administração ou nós de gateway?
- Alguma tarefa foi iniciada e pode levar muito tempo para ser concluída? Exemplos incluem:
  - Recuperação de um nó de armazenamento com falha
  - Descomissionamento do nó de armazenamento
- Alguma alteração foi feita na autenticação do usuário, como adicionar um locatário ou alterar a configuração do LDAP?
- A migração de dados está ocorrendo?
- Os serviços da plataforma foram habilitados ou alterados recentemente?
- A conformidade foi ativada recentemente?
- Os pools de armazenamento em nuvem foram adicionados ou removidos?
- Alguma alteração foi feita na compactação ou criptografia do armazenamento?
- Houve alguma mudança na infraestrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Alguma alteração foi feita nas fontes NTP?
- Foram feitas alterações nas interfaces de rede Grid, Admin ou Client Network?
- Alguma outra alteração foi feita no sistema StorageGRID ou em seu ambiente?

Estabelecer linhas de base

Você pode estabelecer linhas de base para seu sistema registrando os níveis normais de vários valores operacionais. No futuro, você poderá comparar os valores atuais com essas linhas de base para ajudar a detectar e resolver valores anormais.

Propriedade	Valor	Como obter
Consumo médio de armazenamento	GB consumidos/dia Porcentagem consumida/dia	Acesse o Gerenciador de Grade. Na página Nós, selecione a grade inteira ou um site e vá para a guia Armazenamento. No gráfico Armazenamento usado - Dados do objeto, encontre um período em que a linha seja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.
Consumo médio de metadados	GB consumidos/dia Porcentagem consumida/dia	Acesse o Gerenciador de Grade. Na página Nós, selecione a grade inteira ou um site e vá para a guia Armazenamento. No gráfico Armazenamento usado - Metadados do objeto, encontre um período em que a linha seja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.
Taxa de operações S3/Swift	Operações/segundo	No painel do Grid Manager, selecione **Desempenho** > **Operações S3** ou **Desempenho** > **Operações Swift**. Para ver as taxas e contagens de ingestão e recuperação de um site ou nó específico, selecione **NÓS** > ***site ou Nó de Armazenamento*** > **Objetos**. Posicione o cursor sobre o gráfico Ingestão e Recuperação do S3.
Operações S3/Swift com falha	Operações	Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**. Na guia Visão geral na seção Operações da API, visualize o valor para Operações do S3 - Falha ou Operações do Swift - Falha.

Propriedade	Valor	Como obter
Taxa de avaliação do ILM	Objetos/segundo	Na página Nós, selecione ***grid*** > **ILM**. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para a **Taxa de avaliação** do seu sistema.
Taxa de varredura ILM	Objetos/segundo	Selecione **NÓS** > ***grade*** > **ILM**. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para **Taxa de varredura** para seu sistema.
Objetos enfileirados de operações do cliente	Objetos/segundo	Selecione **NÓS** > ***grade*** > **ILM**. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para **Objetos na fila (de operações do cliente)** para seu sistema.
Latência média de consulta	Milissegundos	Selecione **NÓS** > ***Nó de Armazenamento*** > **Objetos**. Na tabela Consultas, visualize o valor de Latência Média.

Analisar dados

Use as informações coletadas para determinar a causa do problema e possíveis soluções.

A análise depende do problema, mas em geral:

- Localize pontos de falha e gargalos usando os alertas.
- Reconstrua o histórico do problema usando o histórico de alertas e gráficos.
- Use gráficos para encontrar anomalias e comparar a situação problemática com a operação normal.

Lista de verificação de informações de escalonamento

Se você não conseguir resolver o problema sozinho, entre em contato com o suporte técnico. Antes de entrar em contato com o suporte técnico, reúna as informações listadas na tabela a seguir para facilitar a resolução do problema.

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, em que horários isso ocorreu? Defina o problema
	Avaliação de impacto	Qual é a gravidade do problema? Qual é o impacto no aplicativo cliente? • O cliente já se conectou com sucesso antes? • O cliente pode ingerir, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione **MANUTENÇÃO** > **Sistema** > **Licença**. O ID do sistema StorageGRID é exibido como parte da licença atual.
	Versão do software	Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Sobre** para ver a versão do StorageGRID .
	Personalização	Resuma como seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grade usa compactação de armazenamento, criptografia de armazenamento ou conformidade? • A ILM cria objetos replicados ou codificados para eliminação? O ILM garante redundância do site? As regras do ILM usam os comportamentos de ingestão Balanceado, Estrito ou Dual Commit?
	Arquivos de log e dados do sistema	Colete arquivos de log e dados do sistema para seu sistema. Selecione **SUPORTE** > **Ferramentas** > **Registros**. Você pode coletar logs para toda a grade ou para nós selecionados. Se você estiver coletando logs apenas para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de armazenamento em um site incluem o serviço ADC.) "Coletar arquivos de log e dados do sistema"
	Informações de base	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabelecer linhas de base

✔	Item	Notas
	Linha do tempo das mudanças recentes	Crie uma linha do tempo que resuma quaisquer alterações recentes no sistema ou em seu ambiente. Crie uma linha do tempo das mudanças recentes
	Histórico de esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, registre as etapas realizadas e o resultado.

Solucionar problemas de objetos e armazenamento

Confirmar a localização dos 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 do ILM está funcionando conforme o esperado e se os dados do objeto estão sendo armazenados onde pretendido.

Antes de começar

- Você deve ter um identificador de objeto, que pode ser um dos seguintes:
  - **UUID**: Identificador Universalmente Único do objeto. Digite o UUID em letras maiúsculas.
  - **CBID**: O identificador exclusivo do objeto dentro do StorageGRID . Você pode obter o CBID de um objeto no log de auditoria. Digite o CBDID em letras maiúsculas.
  - **Chave de bucket e objeto S3**: Quando um objeto é ingerido por meio do"Interface S3" , o aplicativo cliente usa uma combinação de chave de bucket e objeto para armazenar e identificar o objeto.

Passos

1. Selecione **ILM** > **Consulta de metadados do objeto**.
2. Digite o identificador do objeto no campo **Identificador**.

   Você pode inserir um UUID, CBID, chave de objeto/bucket S3 ou nome de objeto/contêiner Swift.

3. Se você quiser consultar uma versão específica do objeto, insira o ID da versão (opcional).

4. Selecione **Procurar**.

   O"resultados da pesquisa de metadados do objeto" aparecer. 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 contêiner, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e a hora em que o objeto foi criado pela primeira vez e a data e a hora em que o objeto foi modificado pela última vez.
   - Quaisquer pares de chave-valor de metadados de usuário personalizados associados ao objeto.
   - Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
   - Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.
   - Para cópias de objetos codificadas por eliminação, o local de armazenamento atual de cada fragmento.
   - Para cópias de objetos em um pool de armazenamento em nuvem, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
   - Para objetos segmentados e objetos multipartes, uma lista de segmentos de objetos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, somente os primeiros 100 segmentos são mostrados.
   - Todos os metadados do objeto no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não têm garantia de persistência de uma versão para outra.

     O exemplo a seguir mostra os resultados da pesquisa de metadados de objeto para um objeto de teste S3 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 de armazenamento de objetos (volume de armazenamento)

O armazenamento subjacente em um nó de armazenamento é dividido em armazenamentos de objetos. Os armazenamentos de objetos também são conhecidos como volumes de armazenamento.

Você pode visualizar informações de armazenamento de objetos para cada nó de armazenamento. Os armazenamentos de objetos são mostrados na parte inferior da página **NODES** > ***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

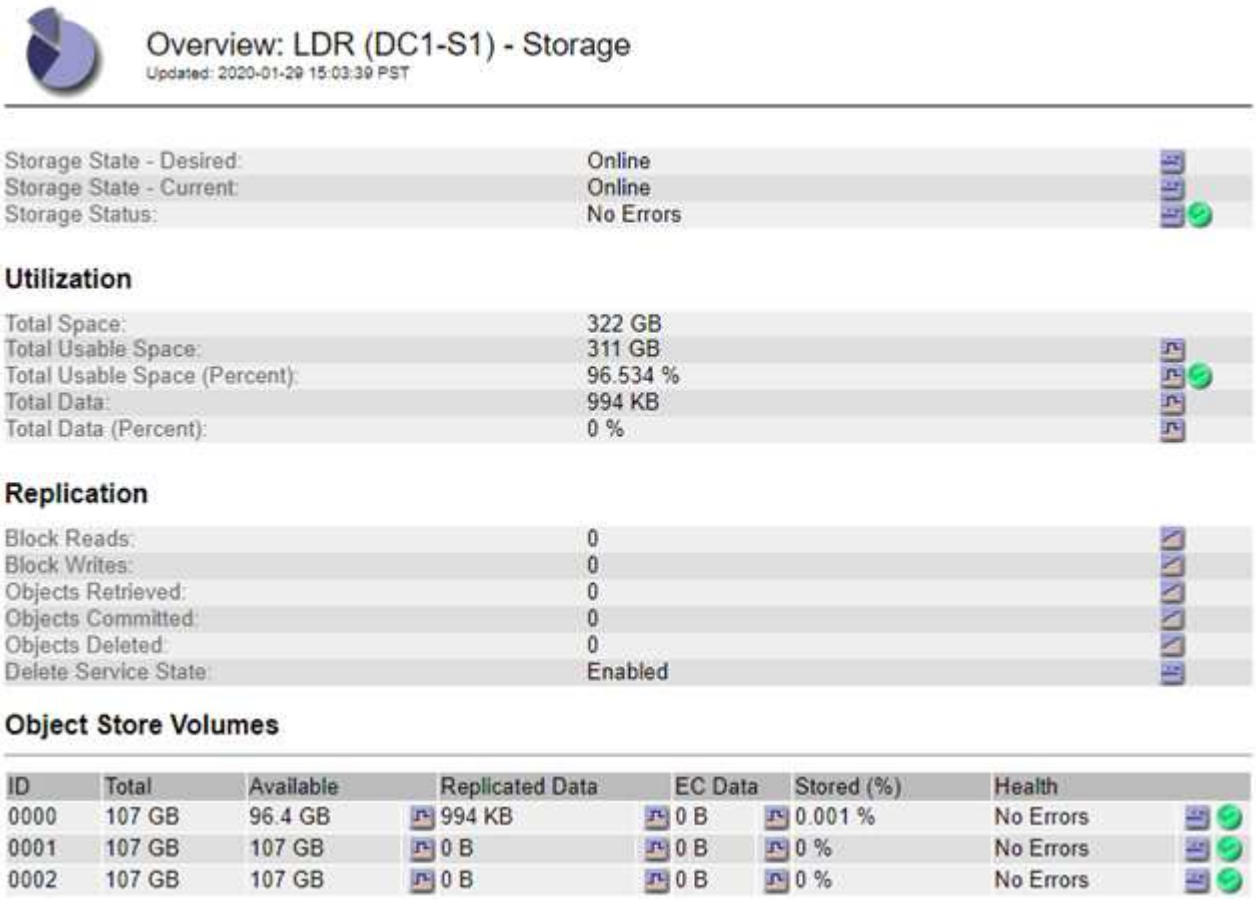
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	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 armazenamento" , siga estes passos:

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***site*** > ***Nó de armazenamento*** > **LDR** > **Armazenamento** > **Visão geral** > **Principal**.



Dependendo da natureza da falha, falhas em um volume de armazenamento podem ser refletidas em"alertas de volume de armazenamento" . Se um volume de armazenamento falhar, você deverá reparar o volume de armazenamento com falha para restaurar o Nó de Armazenamento à funcionalidade completa o mais rápido possível. Se necessário, você pode ir até a aba **Configuração** e"coloque o nó de armazenamento 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.

Verificar integridade do objeto

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

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

O que é verificação de antecedentes?

O processo de verificação em segundo plano verifica automática e continuamente os nós de armazenamento

em busca de cópias corrompidas de dados de objetos e tenta reparar automaticamente quaisquer problemas encontrados.

A verificação de antecedentes verifica a integridade de objetos replicados e objetos codificados para eliminação, da seguinte forma:

- **Objetos replicados**: Se o processo de verificação em segundo plano encontrar um objeto replicado 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 ativas do ILM. A nova cópia pode não ser colocada no nó de armazenamento que foi usado para a cópia original.

  > 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 com codificação de eliminação**: Se o processo de verificação em segundo plano detectar que um fragmento de um objeto com codificação de eliminação está corrompido, o StorageGRID tenta automaticamente reconstruir o fragmento ausente no mesmo nó de armazenamento, usando os dados restantes e os fragmentos de paridade. Se o fragmento corrompido não puder ser reconstruído, será feita uma tentativa de recuperar outra cópia do objeto. Se a recuperação for bem-sucedida, uma avaliação do ILM será realizada para criar uma cópia de substituição do objeto codificado para eliminação.

  O processo de verificação em segundo plano verifica objetos somente em nós de armazenamento. Ele não verifica objetos em um pool de armazenamento em nuvem. Os objetos devem ter mais de quatro dias para se qualificarem para verificação de antecedentes.

A verificação de antecedentes é executada em uma taxa contínua e projetada para não interferir nas atividades normais do sistema. A verificação de antecedentes 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 relacionados à verificação de antecedentes

Se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente (porque a corrupção impede que o objeto seja identificado), o alerta **Objeto corrompido não identificado detectado** será acionado.

Se a verificação de antecedentes não puder substituir um objeto corrompido porque não consegue localizar outra cópia, o alerta **Objetos perdidos** será acionado.

Alterar a taxa de verificação de antecedentes

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

Antes de começar

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

Sobre esta tarefa

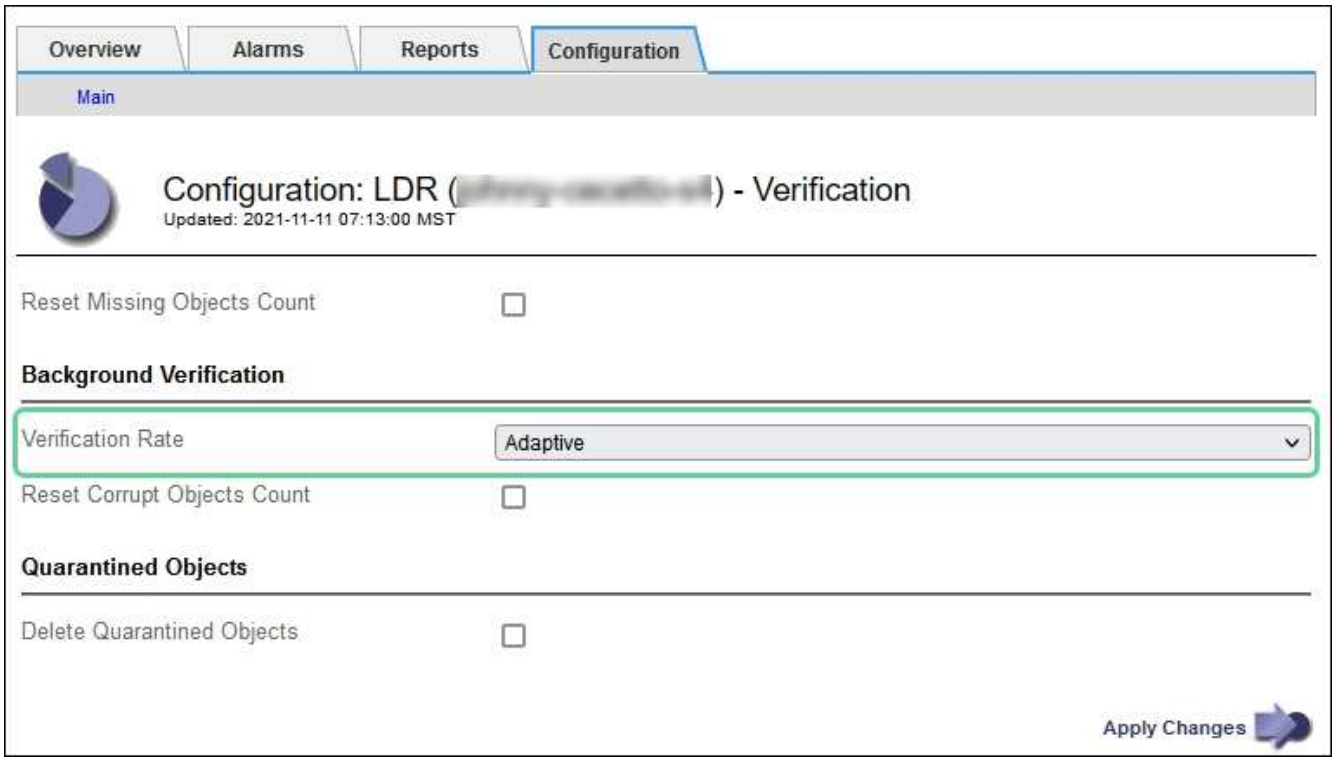
Você pode alterar a Taxa de Verificação para verificação em segundo plano em um Nó de Armazenamento:

- Adaptável: configuração padrão. A tarefa foi projetada para verificar no máximo 4 MB/s ou 10 objetos/s (o que for excedido primeiro).
- Alto: a verificação do armazenamento ocorre rapidamente, a uma taxa que pode retardar as atividades comuns do sistema.

Use a taxa de verificação Alta somente quando suspeitar que uma falha de hardware ou software pode ter corrompido os dados do objeto. Após a conclusão da verificação de antecedentes de alta prioridade, a Taxa de verificação é redefinida automaticamente para Adaptável.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***Nó de armazenamento*** > **LDR** > **Verificação**.
3. Selecione **Configuração** > **Principal**.
4. Vá para **LDR** > **Verificação** > **Configuração** > **Principal**.
5. Em Verificação de antecedentes, selecione **Taxa de verificação** > **Alta** ou **Taxa de verificação** > **Adaptável**.



6. Clique em **Aplicar alterações**.
7. Monitore os resultados da verificação de antecedentes para objetos replicados.
   a. Vá para **NÓS** > ***Nó de Armazenamento*** > **Objetos**.
   b. Na seção Verificação, monitore os valores para **Objetos Corrompidos** e **Objetos Corrompidos Não Identificados**.

      Se a verificação de antecedentes encontrar dados de objetos replicados corrompidos, a métrica **Objetos Corrompidos** será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte maneira:

      - 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 no sistema StorageGRID que satisfaça as políticas de ILM ativas.

- Se o identificador do objeto não puder ser extraído (porque foi corrompido), a métrica **Objetos corrompidos não identificados** será incrementada e o alerta **Objeto corrompido não identificado detectado** será acionado.

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

8. Monitore os resultados da verificação de antecedentes para objetos codificados por eliminação.

   Se a verificação de antecedentes encontrar fragmentos corrompidos de dados de objetos codificados para eliminação, o atributo Fragmentos Corrompidos Detectados será incrementado. O StorageGRID se recupera reconstruindo o fragmento corrompido no mesmo nó de armazenamento.

   a. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
   b. Selecione ***Nó de Armazenamento*** > **LDR** > **Codificação de Apagamento**.
   c. Na tabela Resultados da Verificação, monitore o atributo Fragmentos Corrompidos Detectados (ECCD).

9. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID , redefina a contagem de objetos corrompidos.
   a. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
   b. Selecione ***Nó de armazenamento*** > **LDR** > **Verificação** > **Configuração**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **Aplicar alterações**.

10. Se tiver certeza de que os objetos em quarentena não são necessários, você pode excluí-los.

    > ⓘ Se o alerta **Objetos perdidos** for acionado, o suporte técnico pode querer acessar os objetos em quarentena para ajudar a depurar o problema subjacente ou tentar recuperar os dados.

    a. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
    b. Selecione ***Nó de armazenamento*** > **LDR** > **Verificação** > **Configuração**.
    c. Selecione **Excluir objetos em quarentena**.
    d. Selecione **Aplicar alterações**.

O que é verificação de existência de objetos?

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

Ao contrário da verificação de antecedentes, que ocorre automaticamente, você deve iniciar manualmente um trabalho de verificação de existência de objeto.

A verificação de existência de objetos lê os metadados de cada objeto armazenado no StorageGRID e verifica a existência de cópias de objetos replicadas e fragmentos de objetos codificados para eliminação. Quaisquer dados ausentes são tratados da seguinte forma:

- **Cópias replicadas**: Se uma cópia dos dados do objeto replicado estiver faltando, o StorageGRID tentará automaticamente substituir a cópia por uma cópia armazenada em outro lugar no sistema. O nó de armazenamento executa uma cópia existente por meio de uma avaliação de ILM, que determinará que a política de 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 ausente foi armazenada.
- **Fragmentos codificados por eliminação**: se um fragmento de um objeto codificado por eliminação estiver ausente, o StorageGRID tenta 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 ILM tenta encontrar outra cópia do objeto, que pode ser usada para gerar um novo fragmento codificado por apagamento.

Executar verificação de existência de objeto

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .
- Você garantiu que os nós de armazenamento que deseja verificar estão online. Selecione **NÓS** para visualizar a tabela de nós. Certifique-se de que nenhum ícone de alerta apareça ao lado do nome do nó para os nós que você deseja verificar.
- Você garantiu que os seguintes procedimentos **não** estão em execução nos nós que deseja verificar:
  - Expansão da grade para adicionar um nó de armazenamento
  - Desativação do nó de armazenamento
  - Recuperação de um volume de armazenamento com falha
  - Recuperação de um nó de armazenamento com uma unidade de sistema com falha
  - Reequilíbrio da CE
  - Clone do nó do dispositivo

A verificação de existência do objeto não fornece informações úteis enquanto esses procedimentos estão em andamento.

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 armazenamento selecionados e da consistência selecionada. Você pode executar apenas uma tarefa por vez, mas pode selecionar vários nós de armazenamento e volumes ao mesmo tempo.

Passos

1. Selecione **MANUTENÇÃO** > **Tarefas** > **Verificação de existência de objeto**.
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.

Você não pode selecionar nós que não estejam conectados 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 para o trabalho.

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

   - **Strong-site**: Duas cópias de metadados em um único site.
   - **Strong-global**: Duas cópias de metadados em cada site.
   - **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. Revise e verifique suas seleções. Você pode selecionar **Anterior** para ir para uma etapa anterior no assistente e atualizar suas seleções.

   Um trabalho de verificação de existência de objeto é gerado e executado até que ocorra uma das seguintes situações:

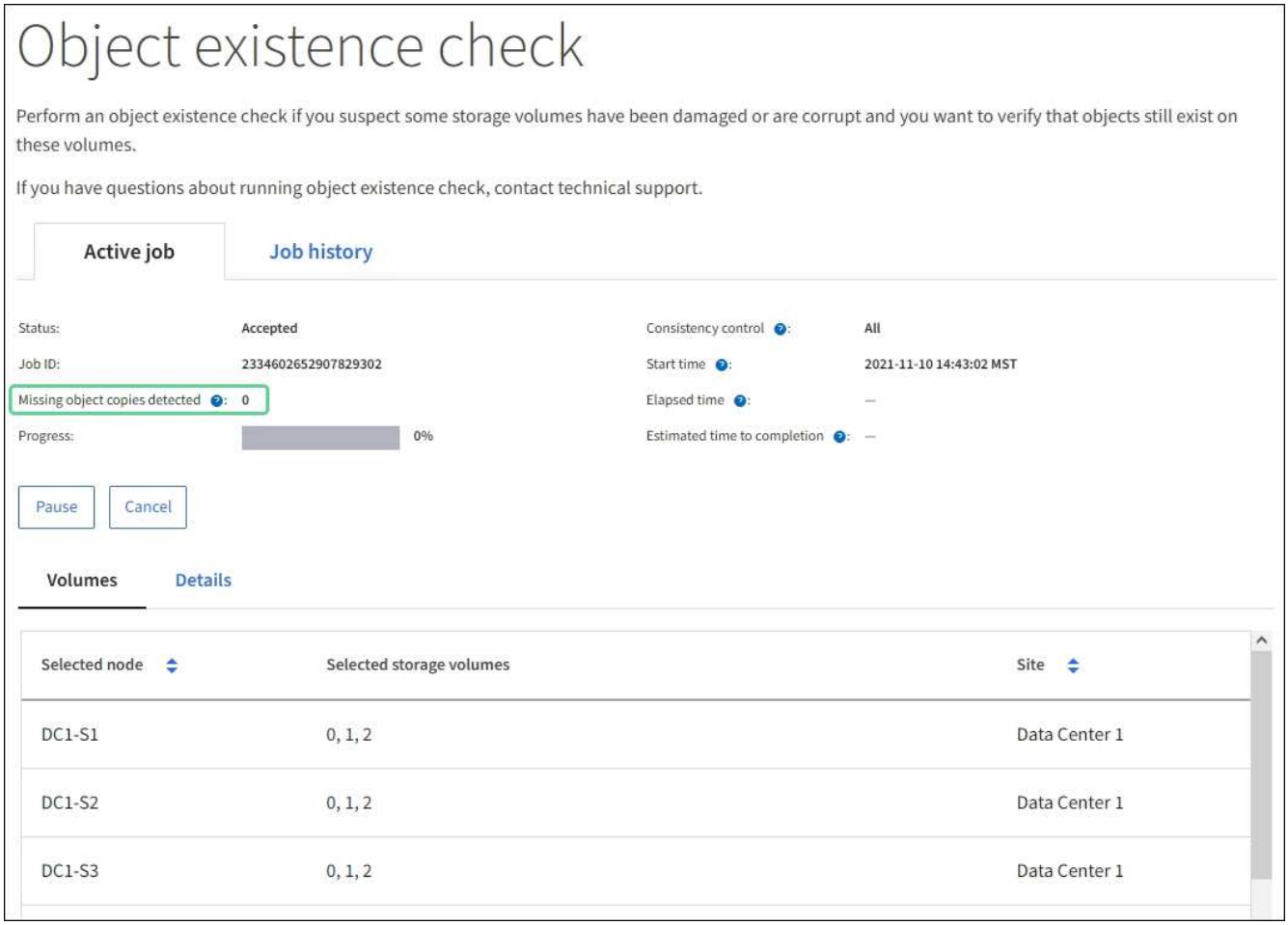
   - O trabalho foi concluído.
   - Você pausa ou cancela o trabalho. Você pode retomar um trabalho que foi pausado, mas não pode retomar um trabalho que foi cancelado.
   - O trabalho estagna. O alerta **A verificação de existência do objeto foi interrompida** é acionado. Siga as ações corretivas especificadas para o alerta.
   - O trabalho falha. O alerta **Falha na verificação de existência do objeto** é acionado. Siga as ações corretivas especificadas para o alerta.
   - Aparece uma mensagem "Serviço indisponível" ou "Erro interno do servidor". Após um minuto, atualize a página para continuar monitorando o trabalho.

   > Conforme necessário, você pode sair da página de verificação de existência do objeto e retornar para continuar monitorando o trabalho.

10. Conforme o trabalho é executado, visualize a guia **Trabalho ativo** e observe o valor de Cópias de objetos ausentes detectadas.

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

    Se o número de cópias de objetos ausentes detectadas 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 o número de cópias de objetos ausentes detectadas for zero, nenhum problema foi encontrado. Nenhuma ação é necessária.
    - Se o número de cópias de objetos ausentes detectadas for maior que zero e o alerta **Objetos perdidos** não tiver sido acionado, todas as cópias ausentes foram reparadas pelo sistema. Verifique se quaisquer problemas de hardware foram corrigidos para evitar danos futuros às cópias de objetos.
    - Se o número de cópias de objetos ausentes detectadas for maior 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 você procure por `LLST` em vez de `OLST` .

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

    Quando o StorageGRID tiver tempo para atingir a consistência de metadados para os nós e volumes incluídos no trabalho, a nova execução do trabalho poderá limpar cópias de objetos ausentes relatadas erroneamente ou fazer com que cópias adicionais de objetos sejam verificadas se estiverem ausentes.

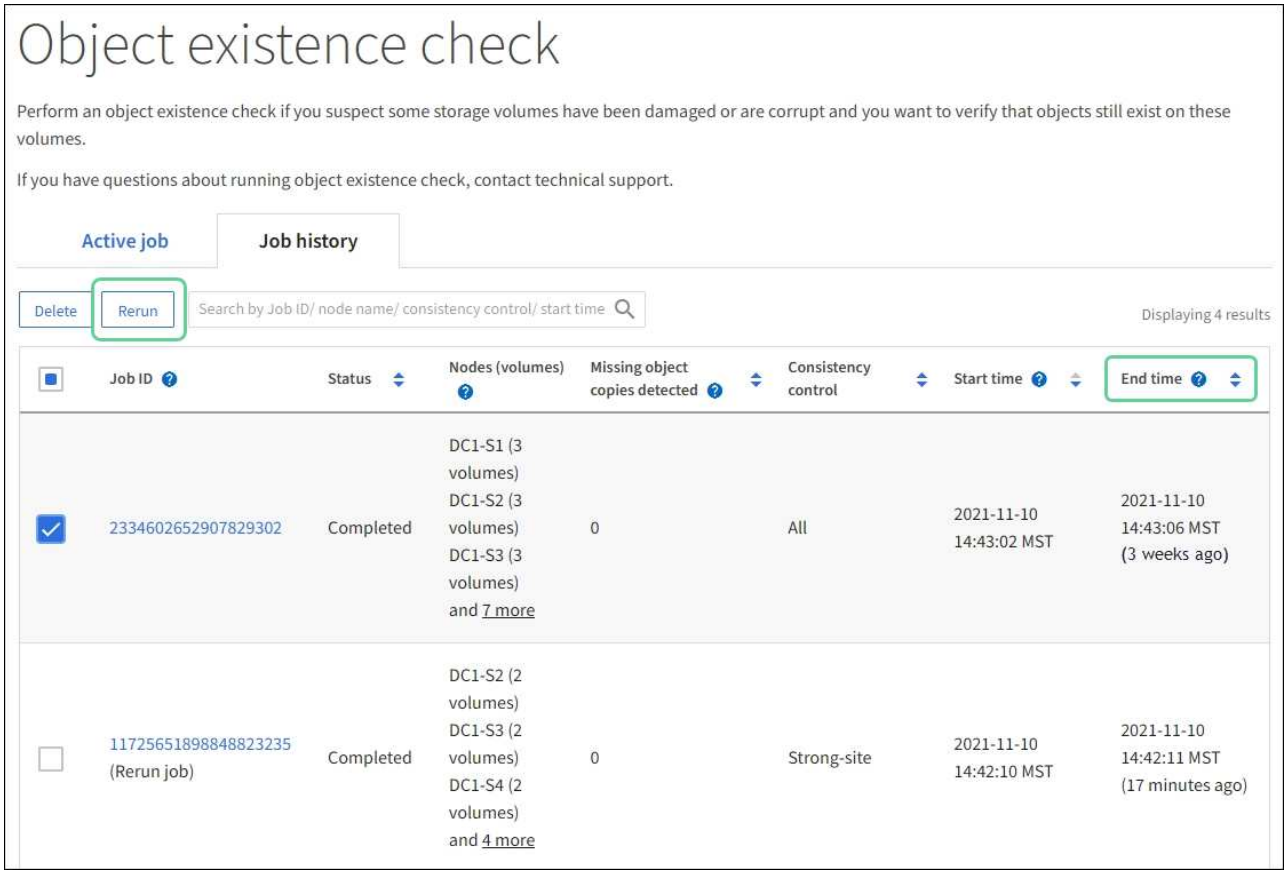
    a. Selecione **MANUTENÇÃO** > **Verificação de existência do objeto** > **Histórico de tarefas**.

b. Determine quais tarefas estão prontas para serem executadas novamente:

   i. Veja a coluna **Hora de término** para determinar quais tarefas foram executadas há mais de três semanas.

   ii. Para esses trabalhos, verifique a coluna Controle de consistência para strong-site ou strong-global.

c. Marque a caixa de seleção de cada tarefa que você deseja executar novamente e selecione **Executar novamente**.



d. No assistente de execução repetida de trabalhos, revise os nós e volumes selecionados e a consistência.

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

A guia Trabalho ativo é exibida. Todos os trabalhos selecionados serão executados novamente como um único trabalho com consistência de strong-site. Um campo **Trabalhos relacionados** na seção Detalhes lista os IDs dos trabalhos originais.

Depois que você terminar

Se você ainda tiver dúvidas sobre a integridade dos dados, vá para **SUPORTE** > **Ferramentas** > **Topologia de grade** > ***site*** > ***Nó de armazenamento*** > **LDR** > **Verificação** > **Configuração** > **Principal** e aumente a Taxa de verificação em segundo plano. A verificação de antecedentes verifica a exatidão de todos os dados de objetos armazenados e repara quaisquer problemas encontrados. Encontrar e reparar possíveis problemas o mais rápido possível reduz o risco de perda de dados.

Solucionar problemas de alerta de tamanho de objeto S3 PUT muito grande

O alerta de tamanho de objeto S3 PUT 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 conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

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

Passos

1. Vá para **CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**.
2. Se as gravações do cliente estiverem normais, acesse o log de auditoria:

   a. Digitar `ssh admin@primary_Admin_Node_IP`

   b. Digite a senha listada no `Passwords.txt` arquivo.

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

   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .

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

   O diretório do 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` o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

   Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

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

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

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

      ii. Para cada mensagem de auditoria nos resultados, observe `S3AI` campo para determinar o ID da conta do locatário. Use os outros campos na 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 identificá-lo:

   a. Vá para **SUPORTE** > **Ferramentas** > **Registros**. 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 para `bycast.log` :

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

   c. Pesquise no log por `method=PUT` e identificar 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 5 GiB e que devem usar uploads multipartes 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

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

O sistema StorageGRID usa informações de localização nos metadados de um objeto para determinar 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 outro lugar no sistema, supondo que a política do ILM contenha uma regra para fazer duas ou mais cópias do objeto.

Se essa recuperação for bem-sucedida, o sistema StorageGRID substituirá a cópia ausente 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 para eliminação, se uma cópia não puder ser recuperada do local esperado, o atributo Cópias Corrompidas Detectadas (ECOR) será incrementado em um antes de uma tentativa de recuperar uma cópia de outro local. Se nenhuma outra cópia for encontrada, o alerta será disparado.

Você deve investigar todos os alertas de **Objetos perdidos** imediatamente para determinar a causa raiz da perda e para determinar se o objeto ainda pode existir em um Nós de Armazenamento offline ou indisponível no momento. Ver "Investigar objetos perdidos" .

No caso de dados de objetos sem cópias serem perdidos, não há solução de recuperação. No entanto, você deve zerar o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos. Ver "Redefinir contagens de objetos perdidos e desaparecidos" .

Investigar objetos perdidos

Quando o alerta **Objetos perdidos** for 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 conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.

Sobre esta tarefa

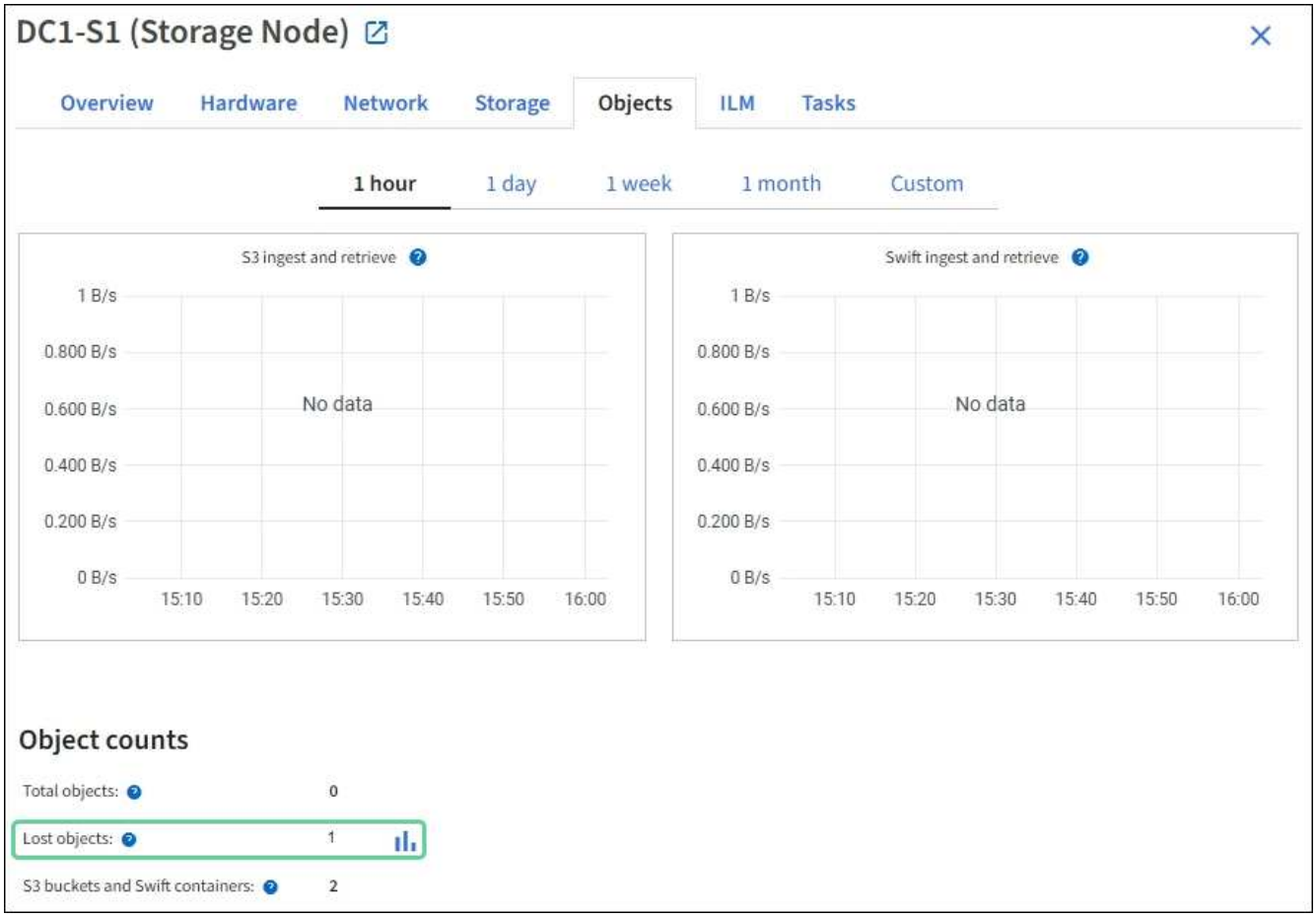
O alerta **Objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

Investigue imediatamente alertas de objetos perdidos. Talvez seja necessário tomar medidas para evitar mais perdas de dados. Em alguns casos, você pode restaurar um objeto perdido se agir rapidamente.

Passos

1. Selecione **NODES**.
2. Selecione ***Nó de Armazenamento*** > **Objetos**.
3. Revise o número de objetos perdidos mostrado na tabela Contagem de objetos.

   Este número indica o número total de objetos que este nó de grade detecta como ausentes em todo o sistema StorageGRID . O valor é a soma dos contadores de objetos perdidos do componente de armazenamento de dados nos serviços LDR e DDS.



4. De um nó de administração,"acessar o log de auditoria" para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **Objetos perdidos**:
   a. Efetue login no nó da grade:
      i. Digite o seguinte comando: `ssh admin@grid_node_IP`
      ii. Digite a senha listada no `Passwords.txt` arquivo.
      iii. Digite o seguinte comando para alternar para root: `su -`
      iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#` .
   b. Mude para o diretório onde os logs de auditoria estão localizados.

      O diretório do 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` o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

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

c. Use grep para extrair as mensagens de auditoria de Objeto Perdido (OLST). Digitar: `grep OLST audit_file_name`

d. Observe o valor do 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. Procure os metadados do objeto perdido usando o UUID:

a. Selecione **ILM** > **Consulta de metadados do objeto**.

b. Digite o UUID e selecione **Procurar**.

c. Revise os locais nos metadados e tome as medidas apropriadas:

Metadados	Conclusão
Objeto <object_identifier> não encontrado	Se o objeto não for encontrado, a mensagem "ERROR":"" será retornada. Se o objeto não for encontrado, você pode zerar a contagem de **Objetos perdidos** para limpar o alerta. A ausência de um objeto indica que o objeto foi excluído intencionalmente.

Metadados	Conclusão
Locais > 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 caminho do arquivo listados na saída para confirmar se o arquivo de objeto está no local listado. (O procedimento para"procurando por objetos potencialmente perdidos" explica como usar o ID do nó para encontrar o nó de armazenamento correto.) Se os objetos existirem, você pode zerar a contagem de **Objetos perdidos** para limpar o alerta.
Locais = 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar"procurar e restaurar o objeto" você mesmo ou entre em contato com o suporte técnico. O suporte técnico pode solicitar que você determine se há um procedimento de recuperação de armazenamento em andamento. Veja as informações sobre"restaurando dados de objetos usando o Grid Manager" e"restaurando dados de objetos para um volume de armazenamento" .

Pesquisar e restaurar objetos potencialmente perdidos

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

Antes de começar

- Você tem o UUID de qualquer objeto perdido, conforme identificado em"Investigar 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 agir imediatamente.

> Entre em contato com o suporte técnico para obter assistência com este procedimento.

Passos

1. Em um nó de administração, pesquise nos logs de auditoria possíveis localizações de objetos:
   a. Efetue login no nó da grade:
      i. Digite o seguinte comando: `ssh admin@grid_node_IP`
      ii. Digite a senha listada no `Passwords.txt` arquivo.

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

iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#` .

b. Altere para o diretório onde os logs de auditoria estão localizados.

O diretório do 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` o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	`/var/local/log/localaudit.log`

Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

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

c. Use grep para extrair o"mensagens de auditoria associadas ao objeto potencialmente perdido" e enviá-los para um arquivo de saída. Digitar: `grep uuid-value audit_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. Digitar: `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
868710831907434 09]]
```

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 do objeto replicado ausente. O valor de NOID é o ID do nó do LDR onde uma cópia do objeto pode ser encontrada.

Se você encontrar a localização de um objeto, poderá restaurá-lo.

a. Encontre o nó de armazenamento associado a este ID de nó LDR. No Grid Manager, selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**. Em seguida, selecione ***Data Center*** > ***Storage Node*** > **LDR**.

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

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

a. Efetue login no nó da grade:

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

ii. Digite a senha listada no `Passwords.txt` arquivo.

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

iv. Digite a senha listada no `Passwords.txt` arquivo.

Quando você está logado como root, o prompt muda 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, insira:

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

Sempre coloque o caminho do arquivo objeto entre aspas simples nos comandos para escapar de quaisquer caracteres especiais.

- Se o caminho do objeto não for encontrado, o objeto será perdido e não poderá 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 StorageGRID.

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

      Por exemplo, insira:

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

      Emitindo o `Object_Found` O comando notifica a grade sobre a 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` o comando falha. Entre em contato com o suporte técnico.
      - Se o objeto foi restaurado com sucesso para 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'
        ```

        Continue com o próximo passo.

4. Se o objeto foi restaurado com sucesso para StorageGRID, verifique se os novos locais foram criados:
   a. Sign in no Grid Manager usando um"navegador da web compatível" .
   b. Selecione **ILM** > **Consulta de metadados do objeto**.
   c. Digite o UUID e selecione **Procurar**.
   d. Revise os metadados e verifique os novos locais.
5. Em um nó de administração, pesquise nos logs de auditoria a mensagem de auditoria ORLM para este objeto para confirmar se o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme necessário.

a. Efetue login no nó da grade:

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

   ii. Digite a senha listada no `Passwords.txt` arquivo.

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

   iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#` .

b. Mude para o diretório onde os logs de auditoria estão localizados. Consultesubetapa 1. b .

c. Use grep para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Digitar: `grep uuid-value audit_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 grep para extrair as mensagens de auditoria do Object Rules Met (ORLM) deste arquivo de saída. Digitar: `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. Encontre 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 do 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. "Redefinir a contagem de objetos perdidos e desaparecidos"no Gerenciador de Grade.

Redefinir contagens de objetos perdidos e desaparecidos

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos registrados foram 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 conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

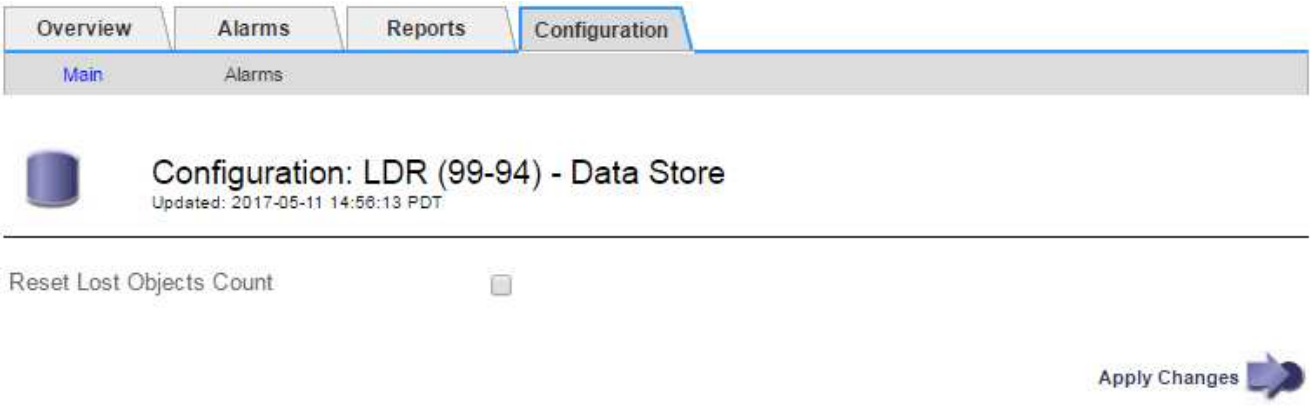
Você pode zerar o contador de Objetos Perdidos em qualquer uma das seguintes páginas:

- **SUPORTE** > **Ferramentas** > **Topologia de grade** > ***Site*** > ***Nó de armazenamento*** > **LDR** > **Armazenamento de dados** > **Visão geral** > **Principal**
- **SUPORTE** > **Ferramentas** > **Topologia de grade** > ***Site*** > ***Nó de armazenamento*** > **DDS** > **Armazenamento de dados** > **Visão geral** > **Principal**

Estas instruções mostram como redefinir o contador na página **LDR** > **Data Store**.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***Site*** > ***Nó de Armazenamento*** > **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 atributos relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.

   a. Selecione ***Site*** > ***Nó de Armazenamento*** > **LDR** > **Codificação de Apagamento** > **Configuração**.

   b. Selecione **Redefinir contagem de falhas de leitura** e **Redefinir contagem de cópias corrompidas detectadas**.

   c. Clique em **Aplicar alterações**.

   d. Selecione ***Site*** > ***Nó de Armazenamento*** > **LDR** > **Verificação** > **Configuração**.

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

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

   Objetos em quarentena são criados quando a verificação em segundo plano identifica uma cópia corrompida do objeto replicado. Na maioria dos casos, o StorageGRID substitui automaticamente o objeto corrompido e é seguro excluir os objetos em quarentena. Entretanto, 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 levar alguns instantes para que os atributos sejam redefinidos após você clicar em **Aplicar alterações**.

Solucionar problemas do alerta de armazenamento de dados de objeto baixo

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

Sobre esta tarefa

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

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

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

Nessa condição:

- `storagegrid_storage_utilization_data_bytes`é uma estimativa do tamanho total de dados de objetos replicados e codificados para eliminação para um nó de armazenamento.
- `storagegrid_storage_utilization_usable_space_bytes`é a quantidade total de espaço de armazenamento de objetos restante para um nó de armazenamento.

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

Passos

1. Selecione **ALERTAS** > **Atual**.

   A página Alertas é exibida.

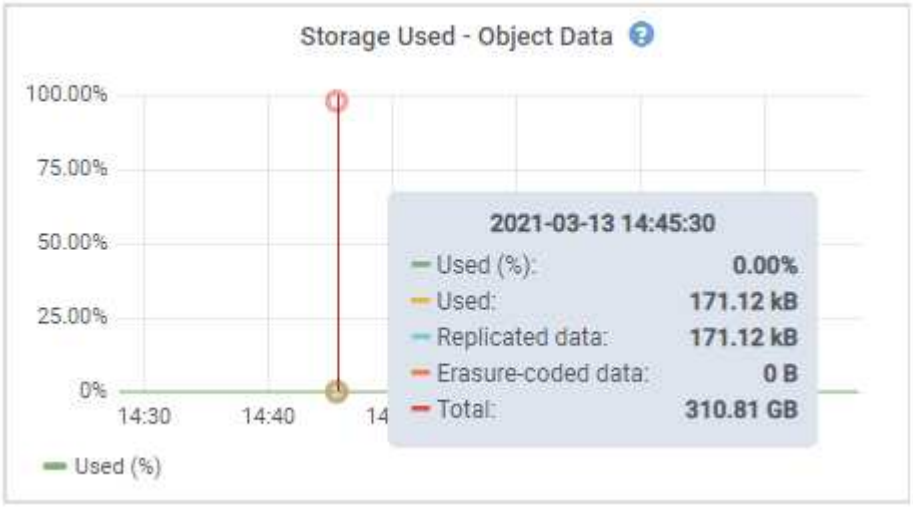
2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja visualizar.

Selecione o alerta, não o título 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** > ***Nó ou Site de Armazenamento*** > **Armazenamento**.
5. Posicione o cursor sobre o gráfico Armazenamento usado - Dados do objeto.

   Os seguintes valores são mostrados:

   - **Usado (%)**: A porcentagem do espaço total utilizável que foi usada para dados do objeto.
   - **Usado**: A quantidade de espaço total utilizável que foi usada para dados do objeto.
   - **Dados replicados**: Uma estimativa da quantidade de dados de objetos replicados neste nó, site ou grade.
   - **Dados codificados por eliminação**: Uma estimativa da quantidade de dados de objetos codificados por eliminação neste nó, site ou grade.
   - **Total**: A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é o `storagegrid_storage_utilization_data_bytes` métrica.



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

   Analisar o uso do armazenamento ao longo do tempo pode ajudar você a entender quanto armazenamento foi usado antes e depois do alerta ser disparado e pode ajudar você a estimar quanto tempo pode levar para o espaço restante do nó ficar cheio.

7. O mais breve possível,"adicionar capacidade de armazenamento" para sua grade.

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

   Para obter mais informações, consulte "Gerenciar nós de armazenamento completos" .

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

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

Em lançamentos anteriores, os três"marcas d'água de volume de armazenamento" eram configurações globais — 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.

Ao atualizar para o StorageGRID 11.6 ou superior, marcas d'água otimizadas somente leitura e leitura/gravação são aplicadas automaticamente a todos os volumes de armazenamento, a menos que uma das seguintes condições seja verdadeira:

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

Entenda o alerta

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

Cada instância do alerta indica que o valor personalizado da marca d'água somente leitura do volume de armazenamento é menor que o valor mínimo otimizado para esse nó de armazenamento. Se você continuar a usar a configuração personalizada, o Nó de Armazenamento poderá ficar com pouco espaço antes de poder fazer a transição segura 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 a marca d'água somente leitura do volume de armazenamento para 5 GB. Agora suponha que o StorageGRID tenha calculado 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 **Substituição de marca d'água somente leitura baixa** é acionado para o Nó de Armazenamento A porque sua marca d'água personalizada (5 GB) é menor que o valor mínimo otimizado para todos os volumes

naquele nó (11 GB). Se você continuar usando a configuração personalizada, o nó poderá ficar com pouco espaço antes de poder fazer a transição segura para o estado somente leitura.

Resolva o alerta

Siga estas etapas se um ou mais alertas de **Substituição de marca d'água somente leitura baixa** tiverem sido acionados. Você também pode usar estas instruções se atualmente usa configurações de marca d'água personalizadas e deseja começar a usar configurações otimizadas mesmo que nenhum alerta tenha sido acionado.

Antes de começar

- Você concluiu a atualização para o StorageGRID 11.6 ou superior.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

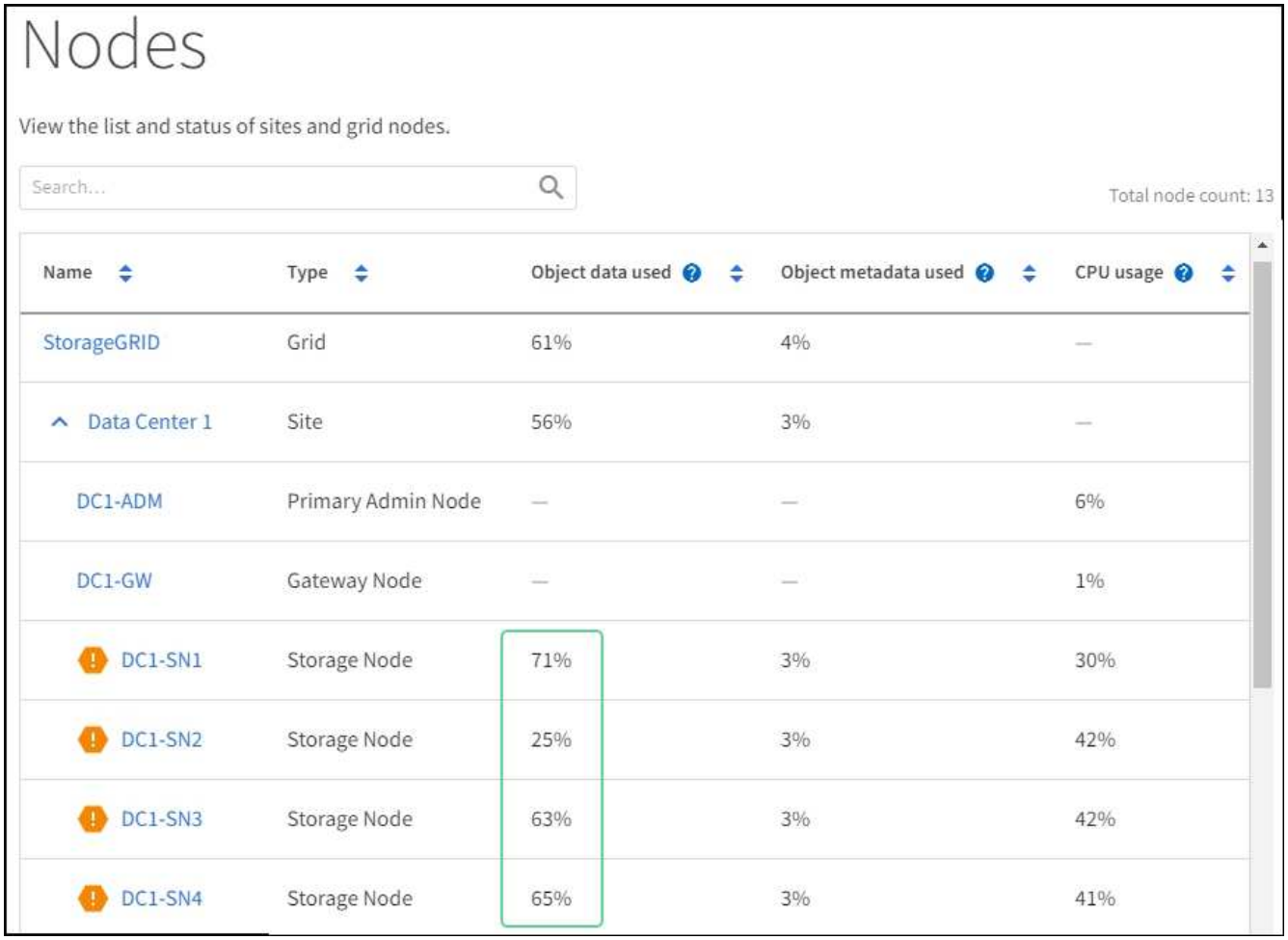
Sobre esta tarefa

Você pode resolver o alerta **Substituição de marca d'água somente leitura baixa** atualizando as configurações de marca d'água personalizadas para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem quase cheios 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 do objeto para toda a grade

Passos

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



4. Siga o passo apropriado:
   a. Se nenhum dos nós de armazenamento estiver quase cheio (por exemplo, todos os valores de **Dados do objeto usados** forem inferiores a 80%), você poderá começar a usar as configurações de substituição. Vá paraUse marcas d'água otimizadas .
   b. Se as regras do ILM usarem o comportamento de ingestão estrito ou se pools de armazenamento específicos estiverem quase cheios, execute as etapas emExibir marcas d'água de armazenamento otimizadas eDetermine se você pode usar marcas d'água otimizadas .

Ver marcas d'água de armazenamento otimizadas

O StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que ele calculou para a marca d'água somente leitura do volume de armazenamento. Você pode visualizar os valores mínimos e máximos otimizados para cada nó de armazenamento na sua grade.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Métricas**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário do Prometheus.
3. Para ver a marca d'água mínima recomendada somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor mínimo otimizado da marca d'água somente leitura para todos os volumes

de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para a marca d'água somente leitura do volume de armazenamento, o alerta **Substituição de marca d'água somente leitura baixa** será acionado para o Nó de Armazenamento.

4. Para ver a marca d'água máxima recomendada para somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor máximo otimizado da marca d'água somente leitura para todos os volumes de armazenamento em cada nó de armazenamento.

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

Determine se você pode usar marcas d'água otimizadas

Passos

1. Selecione **NODES**.
2. Repita estas etapas para cada nó de armazenamento on-line:
   a. Selecione ***Nó de armazenamento*** > **Armazenamento**.
   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 on-line tiver mais espaço disponível do que a marca d'água otimizada máxima para esse nó, vá paraUse marcas d'água otimizadas para começar a usar as marcas d'água otimizadas.

   Caso contrário, expanda a grade o mais rápido possível. Qualquer"adicionar volumes de armazenamento" para um nó existente ou"adicionar novos nós de armazenamento" . Então vá paraUse marcas d'água otimizadas para atualizar as configurações da marca d'água.

4. Se você precisar continuar usando valores personalizados para as marcas d'água do volume de armazenamento,"silêncio" ou"desabilitar" o alerta **Substituição 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. Usar valores menores que os recomendados para marcas d'água de volume de armazenamento pode fazer com que alguns volumes de armazenamento se tornem inacessíveis (desmontados automaticamente) quando o nó atingir a capacidade.

Use marcas d'água otimizadas

Passos

1. Vá para **SUPORTE** > **Outros** > **Marcas d'água de armazenamento**.
2. Marque a caixa de seleção **Usar valores otimizados**.
3. Selecione **Salvar**.

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

Solucionar problemas de metadados

Se ocorrerem problemas de metadados, os alertas informarão a origem dos problemas e as ações recomendadas a serem tomadas. Em particular, você deve adicionar novos nós de armazenamento se o alerta de armazenamento de metadados baixo for acionado.

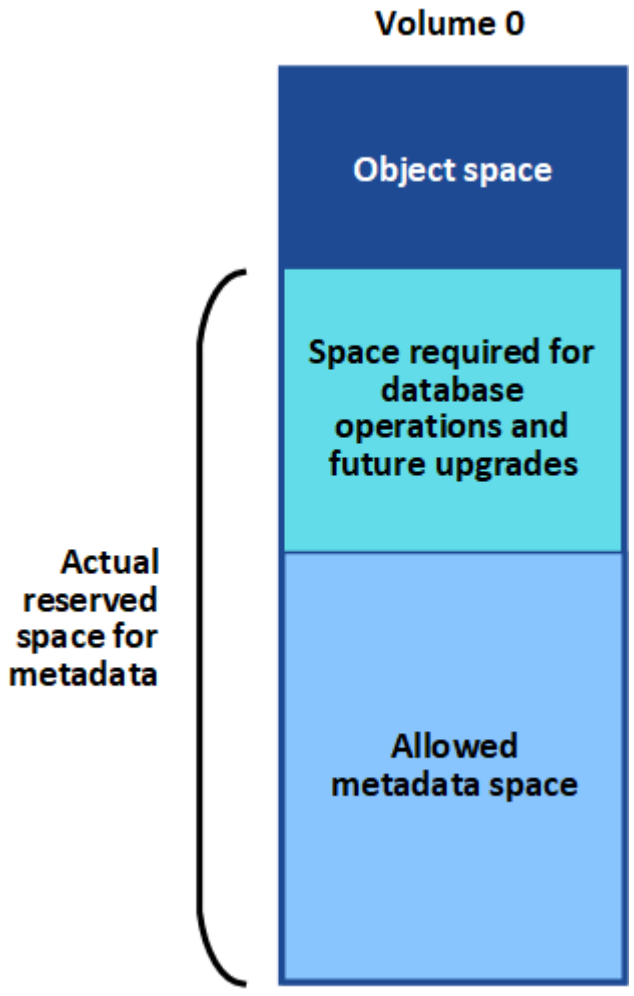
Antes de começar

Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Siga as ações recomendadas para cada alerta relacionado a metadados que for acionado. Se o alerta **Armazenamento de metadados baixo** for acionado, você deverá adicionar novos Nós de Armazenamento.

O StorageGRID reserva uma certa quantidade de espaço no volume 0 de cada nó de armazenamento para metadados de objetos. Este espaço, conhecido como *espaço reservado real*, é subdividido no espaço permitido para metadados de objetos (o espaço de metadados permitido) e no espaço necessário para operações essenciais do banco de dados, como compactação e reparo. O espaço de metadados permitido controla a capacidade geral do objeto.



Se os metadados do objeto consumirem mais de 100% do espaço permitido para metadados, as operações do banco de dados não poderão ser executadas com eficiência e ocorrerão erros.

Você pode"monitorar a capacidade de metadados do objeto para cada nó de armazenamento" para ajudar

você a antecipar erros e corrigi-los antes que eles ocorram.

O StorageGRID usa a seguinte métrica do Prometheus para medir o quão cheio está o espaço de metadados permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Quando essa expressão do Prometheus atinge certos limites, o alerta **Armazenamento de metadados baixo** é acionado.

- **Menor**: Os metadados do objeto estão usando 70% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de armazenamento o mais rápido possível.
- **Principal**: Os metadados do objeto estão usando 90% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de armazenamento imediatamente.

> Quando os metadados do objeto estão usando 90% ou mais do espaço de metadados permitido, um aviso aparece no painel. Se esse aviso aparecer, você deverá adicionar novos Nós de Armazenamento imediatamente. Você nunca deve permitir que metadados de objetos usem mais de 100% do espaço permitido.

- **Crítico**: Os metadados do objeto estão usando 100% ou mais do espaço de metadados permitido e estão começando a consumir o espaço necessário para operações essenciais do banco de dados. Você deve interromper a ingestão de novos objetos e adicionar novos Nós de Armazenamento imediatamente.

> Se o tamanho do volume 0 for menor que a opção de armazenamento Espaço Reservado de Metadados (por exemplo, em um ambiente de não produção), o cálculo do alerta **Armazenamento de metadados baixo** poderá ser impreciso.

Passos

1. Selecione **ALERTAS** > **Atual**.
2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de metadados baixo**, se necessário, e selecione o alerta específico que deseja visualizar.
3. Revise os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **Baixo armazenamento de metadados** for acionado, execute uma expansão para adicionar nós de armazenamento imediatamente.

> Como o StorageGRID mantém cópias completas de todos os metadados do objeto em cada site, a capacidade de metadados de toda a grade é limitada pela capacidade de metadados do menor site. Se você precisar adicionar capacidade de metadados a um site, você também deve"expandir quaisquer outros sites" pelo mesmo número de nós de armazenamento.

Depois de executar a expansão, o StorageGRID redistribui os metadados do objeto existentes para os novos nós, o que aumenta a capacidade geral de metadados da grade. Nenhuma ação do usuário é necessária. O alerta **Baixo armazenamento de metadados** foi removido.

Solucionar erros de certificado

Se você observar um problema de segurança ou de certificado ao tentar se conectar ao StorageGRID usando um navegador da Web, um cliente S3 ou uma ferramenta de monitoramento externa, verifique o certificado.

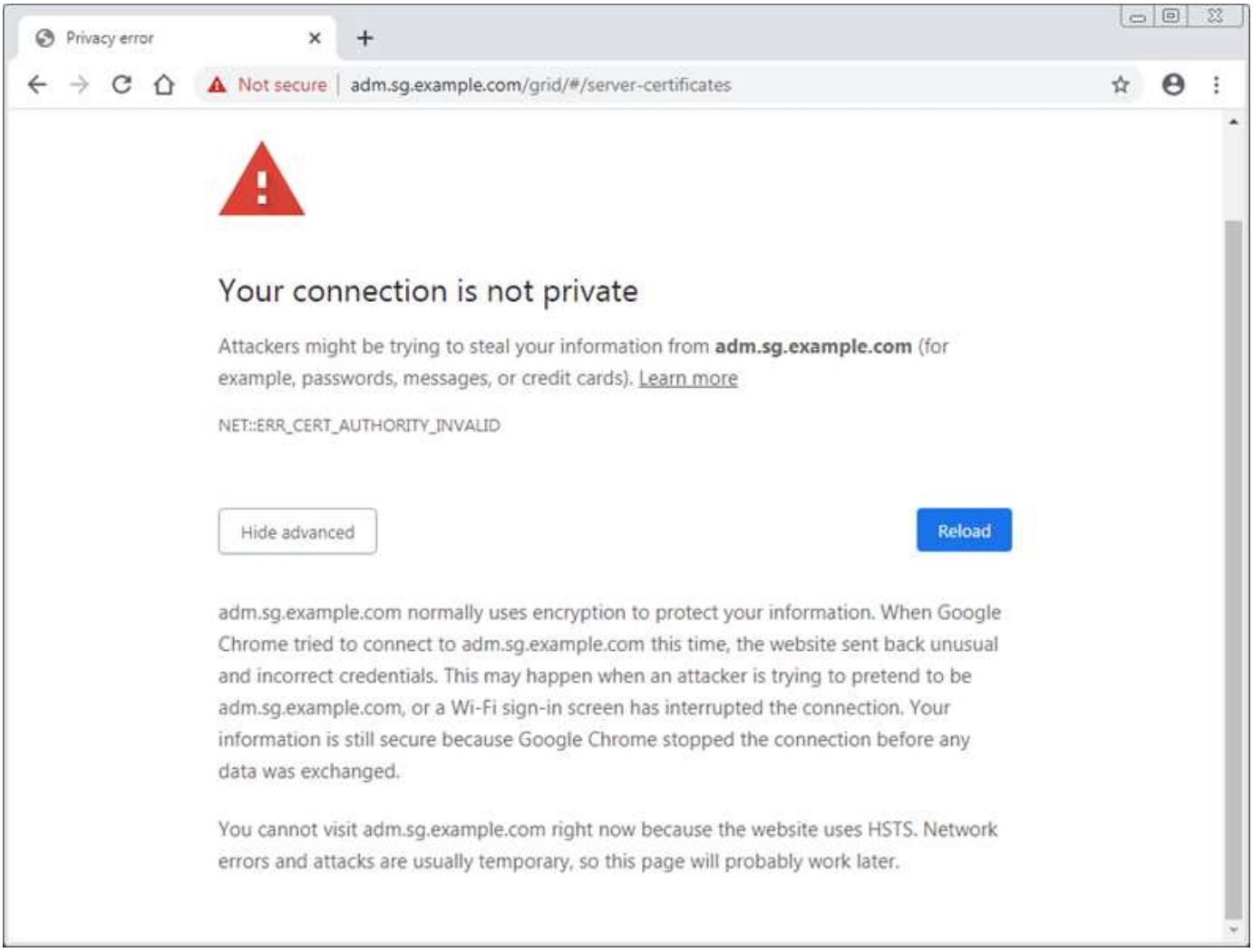
Sobre esta tarefa

Erros de certificado podem causar problemas quando você tenta se conectar ao StorageGRID usando o Grid Manager, a Grid Management API, o Tenant Manager ou a Tenant Management API. Erros de certificado também podem ocorrer quando você tenta se conectar a um cliente S3 ou a uma ferramenta de monitoramento externa.

Se você estiver acessando o Grid Manager ou o Tenant Manager usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se ocorrer qualquer uma das seguintes situações:

- Seu certificado de interface de gerenciamento personalizado expira.
- Você reverte de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão.

O exemplo a seguir mostra um erro de certificado quando o certificado da interface de gerenciamento personalizada expirou:



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado do servidor para a Interface de Gerenciamento** é acionado quando o certificado do servidor está prestes a expirar.

Ao usar certificados de cliente para integração externa do Prometheus, erros de certificado podem ser causados pelo certificado da interface de gerenciamento do StorageGRID ou por certificados de cliente. O alerta **Expiração de certificados de cliente configurados na página Certificados** é acionado quando um certificado de cliente está prestes a expirar.

Passos

Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado: . Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então"selecione a aba de certificado apropriada" .

1. Verifique o período de validade do certificado. + Alguns navegadores da Web e clientes S3 não aceitam certificados com período de validade superior a 398 dias.
2. Se o certificado expirou ou irá expirar em breve, carregue ou gere um novo certificado.
   - Para um certificado de servidor, consulte as etapas para"configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager" .
   - Para um certificado de cliente, consulte as etapas para"configurando um certificado de cliente" .
3. Para erros de certificado de servidor, tente uma ou ambas as opções a seguir:
   - Certifique-se de que o Nome Alternativo do Assunto (SAN) do certificado esteja preenchido e que o SAN corresponda ao endereço IP ou nome do host do nó ao qual você está se conectando.
   - Se você estiver tentando se conectar ao StorageGRID usando um nome de domínio:
     i. Digite o endereço IP do nó de administração em vez do nome de domínio para ignorar o erro de conexão e acessar o Grid Manager.
     ii. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então"selecione a aba de certificado apropriada" para instalar um novo certificado personalizado ou continuar com o certificado padrão.
     iii. Nas instruções para administrar o StorageGRID, veja as etapas para"configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager" .

Solucionar problemas do nó de administração e da interface do usuário

Você pode executar várias tarefas para ajudar a determinar a origem dos problemas relacionados aos nós de administração e à interface do usuário do StorageGRID .

Erros de login do nó de administração

Se você tiver um erro ao fazer login em um nó de administração do StorageGRID , seu sistema pode ter um problema com um"rede" ou "ferragens" problema, uma questão com"Serviços do nó de administração" , ou um"problema com o banco de dados Cassandra" em nós de armazenamento conectados.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o `Passwords.txt` arquivo.

- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

Use estas diretrizes de solução de problemas se você vir alguma das seguintes mensagens de erro ao tentar fazer login em um nó de administração:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Passos

1. Aguarde 10 minutos e tente fazer login novamente.

   Se o erro não for resolvido automaticamente, vá para a próxima etapa.

2. Se o seu sistema StorageGRID tiver mais de um nó de administração, tente fazer login no Grid Manager de outro nó de administração para verificar o status de um nó de administração indisponível.
   - Se você conseguir fazer login, poderá usar as opções **Painel**, **NÓS**, **Alertas** e **SUPORTE** para ajudar a determinar a causa do erro.
   - Se você tiver apenas um nó de administração ou ainda não conseguir fazer login, vá para a próxima etapa.
3. Determine se o hardware do nó está offline.
4. Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , consulte as etapas para"configurando logon único" .

   Pode ser necessário desabilitar e reabilitar temporariamente o SSO para um único nó de administração para resolver quaisquer problemas.

   > ⓘ Se o SSO estiver habilitado, você não poderá fazer logon usando uma porta restrita. Você deve usar a porta 443.

5. Determine se a conta que você está usando pertence a um usuário federado.

   Se a conta de usuário federada não estiver funcionando, tente entrar no Grid Manager como um usuário local, como root.

   - Se o usuário local puder efetuar login:
     i. Revisar alertas.
     ii. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Federação de identidade**.
     iii. Clique em **Testar conexão** para validar suas configurações de conexão para o servidor LDAP.
     iv. Se o teste falhar, resolva quaisquer erros de configuração.
   - Se o usuário local não conseguir fazer login e você tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.
6. Use o Secure Shell (ssh) para efetuar login no nó de administração:

a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`

b. Digite a senha listada no `Passwords.txt` arquivo.

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

d. Digite a senha listada no `Passwords.txt` arquivo.

Quando você está logado como root, o prompt muda de `$` para `#` .

7. Visualize o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços de API nms, mi, nginx e mgmt estejam todos em execução.

A saída é atualizada imediatamente se o status de um serviço mudar.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Confirme se o serviço nginx-gw está em execução `# service nginx-gw status`

9. Use o Lumberjack para coletar toras: `# /usr/local/sbin/lumberjack.rb`

   Se a autenticação com falha ocorreu no passado, você pode usar as opções de script --start e --end do Lumberjack para especificar o intervalo de tempo apropriado. Use lumberjack -h para obter detalhes sobre essas opções.

   A saída para o terminal indica onde o arquivo de log foi copiado.

10. Revise os seguintes logs:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. Se você não conseguir identificar nenhum problema com o nó de administração, emita um dos seguintes comandos para determinar os endereços IP dos três nós de armazenamento que executam o serviço ADC no seu site. Normalmente, esses são os três primeiros nós de armazenamento instalados no local.

    ```
    # cat /etc/hosts
    ```

    ```
    # gpt-list-services adc
    ```

    Os nós de administração usam o serviço ADC durante o processo de autenticação.

12. No nó de administração, use ssh para efetuar login em cada um dos nós de armazenamento do ADC, usando os endereços IP que você identificou.
13. Visualize o status de todos os serviços em execução no nó da grade: `storagegrid-status`

    Certifique-se de que os serviços idnt, acct, nginx e cassandra estejam todos em execução.

14. Repita os passosUse o Lenhador para coletar toras eRegistros de revisão para revisar os logs nos nós de armazenamento.
15. Se você não conseguir resolver o problema, entre em contato com o suporte técnico.

    Forneça os logs coletados ao suporte técnico. Veja também "Referência de arquivos de log" .

Problemas de interface do usuário

A interface do usuário do Grid Manager ou do Tenant Manager pode não responder conforme o esperado após a atualização do software StorageGRID .

Passos

1. Certifique-se de que você está usando um"navegador da web compatível" .
2. Limpe o cache do seu navegador.

   Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário opere corretamente novamente. Para obter instruções, consulte a

documentação do seu navegador.

Solucionar problemas de rede, hardware e plataforma

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas relacionados à rede, hardware e plataforma do StorageGRID .

Erros "422: Entidade não processável"

O erro 422: Entidade não processável pode ocorrer por diferentes motivos. Verifique a mensagem de erro para determinar o que causou o problema.

Se você vir uma das mensagens de erro listadas, tome a ação recomendada.

Mensagem de erro	Causa raiz e ação corretiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password:`
`LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Esta mensagem pode ocorrer se você selecionar a opção **Não usar TLS** para Segurança da Camada de Transporte (TLS) ao configurar a federação de identidade usando o Windows Active Directory (AD).
	
	O uso da opção **Não usar TLS** não é suportado para uso com servidores AD que impõem assinatura LDAP. Você deve selecionar a opção **Usar STARTTLS** ou a opção **Usar LDAPS** para TLS.

Mensagem de erro	Causa raiz e ação corretiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed`
`(EOF)`
	Esta mensagem aparece se você tentar usar uma cifra não suportada para fazer uma conexão TLS (Transport Layer Security) do StorageGRID para um sistema externo usado para identificar federações ou pools de armazenamento em nuvem.
	
	Verifique as cifras oferecidas pelo sistema externo. O sistema deve utilizar um dos"cifras suportadas pelo StorageGRID" para conexões TLS de saída, conforme mostrado nas instruções para administrar o StorageGRID.

Alerta de incompatibilidade de MTU da rede de grade

O alerta **Incompatibilidade de MTU da rede de grade** é acionado quando a configuração da unidade máxima de transmissão (MTU) para a interface da rede de grade (eth0) difere significativamente entre os nós da grade.

Sobre esta tarefa

As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 estão configuradas para quadros jumbo. Uma incompatibilidade de tamanho de MTU maior que 1000 pode causar problemas de desempenho de rede.

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
   - Use a consulta fornecida no Grid Manager.
   - Navegar para *`primary Admin Node IP address`*`/metrics/graph` e insira a seguinte consulta: `node_network_mtu_bytes{device="eth0"}`
2. "Modificar as configurações de MTU"conforme necessário para garantir que sejam os mesmos para a interface da rede Grid (eth0) em todos os nós.
   - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Exemplo: `change-ip.py -n node 1500 grid admin`

     Observação: Em nós baseados em Linux, se o valor de MTU desejado para a rede no contêiner exceder o valor já configurado na interface do host, você deve primeiro configurar a interface do host para ter o valor de MTU desejado e, em seguida, usar o `change-ip.py` script para alterar o valor de MTU da rede no contêiner.

Use os seguintes argumentos para modificar a MTU em nós baseados em Linux ou VMware.

Argumentos posicionais	Descrição
`mtu`	A MTU a ser definida. Deve estar no intervalo de 1280 a 9216.
`network`	As redes às quais a MTU será aplicada. Inclua um ou mais dos seguintes tipos de rede: • grade • administrador • cliente

+

Argumentos opcionais	Descrição
`-h, - help`	Mostrar a mensagem de ajuda e sair.
`-n node, --node node`	O nó. O padrão é o nó local.

Alerta de erro de quadro de recepção de rede de nó

Alertas de **Erro de quadro de recepção de rede de nó** podem ser causados por problemas de conectividade entre o StorageGRID e seu hardware de rede. Este alerta desaparece sozinho depois que o problema subjacente é resolvido.

Sobre esta tarefa

Os alertas de **Erro de quadro de recepção de rede de nó** podem ser causados pelos seguintes problemas com o hardware de rede que se conecta ao StorageGRID:

- A correção de erros antecipada (FEC) é necessária e não está em uso
- Incompatibilidade de porta do switch e MTU da placa de rede
- Altas taxas de erro de link
- Estouro do buffer de anel da placa de rede

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas desse alerta, de acordo com sua configuração de rede.
2. Execute as seguintes etapas dependendo da causa do erro:

Incompatibilidade de FEC

Essas etapas são aplicáveis somente para alertas de **Erro de quadro de recepção de rede de nó** causados por incompatibilidade de FEC em dispositivos StorageGRID .

a. Verifique o status FEC da porta no switch conectado ao seu dispositivo StorageGRID .
b. Verifique a integridade física dos cabos do aparelho até o switch.
c. Se você quiser alterar as configurações do FEC para tentar resolver o alerta, primeiro certifique-se de que o dispositivo esteja configurado para o modo **Automático** na página Configuração de link do instalador do dispositivo StorageGRID (consulte as instruções para seu dispositivo:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 e SG1100"
   - "SG100 e SG1000"
d. Altere as configurações de FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações de FEC para corresponder, se possível.

   Não é possível configurar as definições do FEC em dispositivos StorageGRID . Em vez disso, os dispositivos tentam descobrir e espelhar as configurações de FEC nas portas do switch às quais estão conectados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC podem falhar ao negociar uma configuração FEC comum. Sem uma configuração FEC comum, a rede retornará ao modo "sem FEC". Quando o FEC não está habilitado, as conexões ficam mais suscetíveis a erros causados por ruído elétrico.

   Os dispositivos StorageGRID são compatíveis com Firecode (FC) e Reed Solomon (RS) FEC, além de nenhum FEC.

Incompatibilidade de porta do switch e MTU da placa de rede

Se o alerta for causado por uma incompatibilidade de MTU entre a porta do switch e a NIC, verifique se o tamanho da MTU configurado no nó é o mesmo que a configuração de MTU para a porta do switch.

O tamanho da MTU configurado no nó pode ser menor que a configuração na porta do switch à qual o nó está conectado. Se um nó StorageGRID receber um quadro Ethernet maior que sua MTU, o que é possível com essa configuração, o alerta **Erro de quadro de recepção de rede do nó** poderá ser relatado. Se você acredita que isso é o que está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo de suas metas ou requisitos de MTU de ponta a ponta.

Para obter o melhor desempenho da rede, todos os nós devem ser configurados com valores de MTU semelhantes em suas interfaces de rede de grade. O alerta **Incompatibilidade de MTU da rede de grade** é acionado se houver uma diferença significativa nas configurações de MTU da rede de grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Ver Solucionar problemas de alerta de incompatibilidade de MTU da rede de grade para maiores informações.

Veja também "Alterar configuração de MTU" .

Altas taxas de erro de link

a. Habilite o FEC, caso ainda não esteja habilitado.
b. Verifique se o cabeamento da sua rede é de boa qualidade e não está danificado ou conectado incorretamente.
c. Se os cabos não parecerem ser o problema, entre em contato com o suporte técnico.

Você pode notar altas taxas de erro em um ambiente com alto ruído elétrico.

Estouro do buffer de anel da placa de rede

Se o erro for um estouro do buffer de anel da NIC, entre em contato com o suporte técnico.

O buffer de anel pode ser estourado quando o sistema StorageGRID está sobrecarregado e não consegue processar eventos de rede em tempo hábil.

3. Monitore o problema e entre em contato com o suporte técnico se o alerta não for resolvido.

Erros de sincronização de tempo

Você pode ver problemas com a sincronização de tempo na sua grade.

Se você encontrar problemas de sincronização de tempo, verifique se especificou pelo menos quatro fontes NTP externas, cada uma fornecendo uma referência Stratum 3 ou melhor, e se todas as fontes NTP externas estão operando normalmente e são acessíveis pelos seus nós StorageGRID .

Quando"especificando a fonte NTP externa" para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

Linux: Problemas de conectividade de rede

Você pode ver problemas com a conectividade de rede para nós do StorageGRID hospedados em hosts Linux.

Clonagem de endereço MAC

Em alguns casos, problemas de rede podem ser resolvidos usando clonagem de endereço MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereço MAC para cada uma das suas

redes como "true" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contêiner StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções para"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

> Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contêiner StorageGRID pode fazer com que o sistema operacional host fique inacessível se o modo promíscuo não estiver habilitado no hipervisor.

Para obter mais informações sobre como habilitar a clonagem de MAC, consulte as instruções para"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

Modo promíscuo

Se você não quiser usar a clonagem de endereço MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes daqueles atribuídos pelo hipervisor, certifique-se de que as propriedades de segurança nos níveis de switch virtual e grupo de portas estejam definidas como **Aceitar** para Modo Promíscuo, Alterações de Endereço MAC e Transmissões Falsificadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para obter mais informações sobre o uso do Modo Promíscuo, consulte as instruções para"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

Linux: o status do nó é "órfão"

Um nó Linux em estado órfão geralmente indica que o serviço storagegrid ou o daemon do nó StorageGRID que controla o contêiner do nó morreu inesperadamente.

Sobre esta tarefa

Se um nó Linux relatar que está em um estado órfão, você deve:

- Verifique os logs em busca de erros e mensagens.
- Tente iniciar o nó novamente.
- Se necessário, use comandos do mecanismo de contêiner para parar o contêiner do nó existente.
- Reinicie o nó.

Passos

1. Verifique os logs do daemon de serviço e do nó órfão em busca de erros óbvios ou mensagens sobre saída inesperada.
2. Efetue login no host como root ou use uma conta com permissão sudo.
3. Tente iniciar o nó novamente executando o seguinte comando: `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   Se o nó for órfão, a resposta é

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. No Linux, pare o mecanismo de contêiner e quaisquer processos de controle do storagegrid-node. Por exemplo: `sudo docker stop --time secondscontainer-name`

   Para `seconds` , insira o número de segundos que você deseja esperar para que o contêiner pare (normalmente 15 minutos ou menos). Por exemplo:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Reinicie o nó: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Solucionar problemas de suporte a IPv6

Talvez seja necessário habilitar o suporte a IPv6 no kernel se você tiver instalado nós StorageGRID em hosts Linux e perceber que endereços IPv6 não foram atribuídos aos contêineres de nós conforme o esperado.

Sobre esta tarefa

Para ver o endereço IPv6 que foi atribuído a um nó de grade:

1. Selecione **NÓS** e selecione o nó.
2. Selecione **Mostrar endereços IP adicionais** ao lado de **Endereços IP** na guia Visão geral.

Se o endereço IPv6 não for exibido e o nó estiver instalado em um host Linux, siga estas etapas para habilitar o suporte a IPv6 no kernel.

Passos

1. Efetue login no host como root ou use uma conta com permissão sudo.
2. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

   O resultado deve ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

   Se o resultado não for 0, consulte a documentação do seu sistema operacional para alterar `sysctl` configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Digite o contêiner do nó StorageGRID : `storagegrid node enter node-name`

4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> Se o resultado não for 1, este procedimento não se aplica. Entre em contato com o suporte técnico.

5. Sair do contêiner: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite o seguinte arquivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf` .

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localize as duas linhas a seguir e remova as tags de comentário. Em seguida, salve e feche o arquivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Execute estes comandos para reiniciar o contêiner StorageGRID :

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Solucionar problemas de um servidor syslog externo

A tabela a seguir descreve as mensagens de erro que podem estar relacionadas ao uso de um servidor syslog externo e lista as ações corretivas.

Esses erros são exibidos pelo assistente Configurar servidor syslog externo se você tiver problemas para enviar mensagens de teste para validar se o servidor syslog externo está configurado corretamente.

Problemas em tempo de execução podem ser relatados pelo"Erro de encaminhamento do servidor syslog externo" alerta. Se você receber este alerta, siga as instruções no alerta para reenviar as mensagens de teste para que você possa obter mensagens de erro detalhadas.

Para obter mais informações sobre como enviar informações de auditoria para um servidor syslog externo, consulte:

- "Considerações para usar um servidor syslog externo"
- "Configurar mensagens de auditoria e servidor syslog externo"

Mensagem de erro	Descrição e ações recomendadas
Não é possível resolver o nome do host	O FQDN inserido para o servidor syslog não pôde ser resolvido para um endereço IP. 1. Verifique o nome do host que você digitou. Se você inseriu um endereço IP, certifique-se de que seja um endereço IP válido na notação WXYZ ("decimal com ponto"). 2. Verifique se os servidores DNS estão configurados corretamente. 3. Confirme se cada nó pode acessar os endereços IP do servidor DNS.
Ligação recusada	Uma conexão TCP ou TLS com o servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS do host, ou um firewall pode estar bloqueando o acesso. 1. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 2. Confirme se o host do serviço syslog está executando um daemon syslog que está escutando na porta especificada. 3. Confirme se um firewall não está bloqueando o acesso às conexões TCP/TLS dos nós ao IP e à porta do servidor syslog.
Rede inacessível	O servidor syslog não está em uma sub-rede conectada diretamente. Um roteador retornou uma mensagem de falha de ICMP para indicar que não conseguiu encaminhar as mensagens de teste dos nós listados para o servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes da rede de grade, as Listas de sub-redes das redes de administração e os gateways da rede do cliente. Confirme se eles estão configurados para rotear o tráfego para o servidor syslog pela interface de rede e gateway esperados (Grid, Admin ou Cliente).

Mensagem de erro	Descrição e ações recomendadas
Host inacessível	O servidor syslog está em uma sub-rede conectada diretamente (sub-rede usada pelos nós listados para seus endereços IP de grade, administrador ou cliente). Os nós tentaram enviar mensagens de teste, mas não receberam respostas às solicitações ARP para o endereço MAC do servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Verifique se o host que executa o serviço syslog está ativo.
Tempo de conexão esgotado	Uma tentativa de conexão TCP/TLS foi feita, mas nenhuma resposta foi recebida do servidor syslog por um longo tempo. Pode haver uma configuração incorreta de roteamento ou um firewall pode estar descartando tráfego sem enviar nenhuma resposta (uma configuração comum). 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes da rede de grade, as Listas de sub-redes das redes de administração e os gateways da rede do cliente. Confirme se eles estão configurados para rotear o tráfego para o servidor syslog usando a interface de rede e o gateway (Grid, Admin ou Cliente) pelos quais você espera que o servidor syslog seja alcançado. 3. Confirme se um firewall não está bloqueando o acesso às conexões TCP/TLS dos nós listados para o IP e a porta do servidor syslog.
Conexão fechada pelo parceiro	Uma conexão TCP com o servidor syslog foi estabelecida com sucesso, mas foi fechada posteriormente. Os motivos para isso podem incluir: • O servidor syslog pode ter sido reiniciado ou reinicializado. • O nó e o servidor syslog podem ter configurações TCP/TLS diferentes. • Um firewall intermediário pode estar fechando conexões TCP ociosas. • Um servidor não syslog escutando na porta do servidor syslog pode ter fechado a conexão. Para resolver esse problema: 1. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 2. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 3. Verifique se um firewall intermediário não está configurado para fechar conexões TCP ociosas.

Mensagem de erro	Descrição e ações recomendadas
Erro de certificado TLS	O certificado do servidor recebido do servidor syslog não era compatível com o pacote de certificados da CA e o certificado do cliente que você forneceu. 1. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor no servidor syslog. 2. Confirme se as identidades no certificado do servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Encaminhamento suspenso	Os registros do Syslog não estão mais sendo encaminhados para o servidor Syslog e o StorageGRID não consegue detectar o motivo. Revise os logs de depuração fornecidos com este erro para tentar determinar a causa raiz.
Sessão TLS encerrada	O servidor syslog encerrou a sessão TLS e o StorageGRID não consegue detectar o motivo. 1. Revise os logs de depuração fornecidos com este erro para tentar determinar a causa raiz. 2. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 3. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 4. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor do servidor syslog. 5. Confirme se as identidades no certificado do servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Falha na consulta de resultados	O nó de administração usado para configuração e teste do servidor syslog não consegue solicitar resultados de teste dos nós listados. Um ou mais nós podem estar inativos. 1. Siga as etapas padrão de solução de problemas para garantir que os nós estejam online e todos os serviços esperados estejam em execução. 2. Reinicie o serviço miscd nos nós listados.

Informações sobre direitos autorais

Informações sobre marcas comerciais