



Solucionar problemas do sistema StorageGRID

StorageGRID

NetApp
December 03, 2025

Índice

Solucionar problemas do sistema StorageGRID	1
Solucionar problemas de um sistema StorageGRID: Visão geral	1
defina o problema	1
Avaliar o risco e o impactos no sistema	1
Coletar dados	2
Analisaar dados	6
Lista de verificação de informações de encaminhamento	6
Solucionar problemas de objetos e storage	8
Confirmar localizações de dados do objeto	8
Falhas no armazenamento de objetos (volume de storage)	10
Verifique a integridade do objeto	12
Resolução de problemas S3 COLOQUE o alerta tamanho do objeto demasiado grande	20
Solucionar problemas de dados de objetos perdidos e ausentes	22
Solucionar problemas do alerta de armazenamento de dados de objetos baixos	35
Solucionar problemas de alertas de substituição de marca d'água somente leitura baixa	37
Solucione o problema do alarme de Status de armazenamento (SSTS)	41
Solucionar problemas de entrega de mensagens de serviços da plataforma (alarme SMTT)	45
Solucionar problemas de metadados	46
Alerta baixo de armazenamento de metadados	46
Serviços: Status - alarme Cassandra (SVST)	48
Erros de memória sem Cassandra (alarme SMTT)	52
Solucionar erros de certificado	53
Solucionar problemas de nó de administração e interface do usuário	54
Erros de início de sessão	54
Problemas na interface do usuário	58
Nó Admin indisponível	58
Solucionar problemas de rede, hardware e plataforma	59
"422: Entidade não processável" erros	59
Alerta de incompatibilidade da MTU da rede de Grade	60
Alarme de erro de receção de rede (NRER)	61
Erros de sincronização de tempo	64
Linux: Problemas de conetividade de rede	65
Linux: O status do nó é "órfão"	65
Linux: Solucione problemas de suporte ao IPv6	66
Solucionar problemas de um servidor syslog externo	68

Solucionar problemas do sistema StorageGRID

Solucionar problemas de um sistema StorageGRID: Visão geral

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.

Normalmente, você pode resolver problemas sozinho. No entanto, talvez seja necessário encaminhar alguns problemas para o suporte técnico.

defina o problema

O primeiro passo para resolver um problema é definir o problema 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 está fazendo? Quais são seus sintomas?	Os aplicativos clientes estão relatando que os objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez em cerca de 14:50 em 8 de janeiro de 2020.
Como você notou o problema pela primeira vez?	Notificado pela aplicação do cliente. Também recebeu notificações por e-mail de alerta.
O problema acontece de forma consistente, ou apenas às vezes?	O problema está em curso.
Se o problema ocorrer regularmente, quais as etapas que o causam	O problema acontece toda vez que um cliente tenta ingerir um objeto.
Se o problema ocorrer intermitentemente, quando ocorre? Registre os horários de cada incidente que você está ciente.	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 vi esta questão.

Avaliar o risco e o impactos no sistema

Depois de definir o problema, avalie o risco e o impactos no sistema StorageGRID. Por exemplo, a presença de alertas críticos não significa necessariamente que o sistema não está fornecendo serviços básicos.

Esta tabela resume o impactos 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 podem.
Os dados estão em risco?	Não
A capacidade de conduzir negócios é severamente afetada?	Sim, porque os aplicativos cliente 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 o seu risco e impactos, recolha dados para análise. O tipo de dados que é mais útil para coletar depende da natureza do problema.

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Crie a linha do tempo das mudanças recentes	As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.	<ul style="list-style-type: none"> Crie uma linha do tempo das mudanças recentes
Reveja alertas e alarmes	<p>Alertas e alarmes podem ajudá-lo a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso.</p> <p>Revise a lista de alertas e alarmes atuais para ver se o StorageGRID identificou a causa raiz de um problema para você.</p> <p>Reveja alertas e alarmes acionados no passado para obter informações adicionais.</p>	<ul style="list-style-type: none"> "Ver alertas atuais e resolvidos" "Gerenciar alarmes (sistema legado)"
Monitorar eventos	Os 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.	<ul style="list-style-type: none"> "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas apareceram pela primeira vez e podem ajudá-lo a entender a rapidez com que as coisas estão mudando.	<ul style="list-style-type: none"> "Use gráficos e gráficos" "Use relatórios de texto"

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Estabeleça linhas de base	Recolher informações sobre os níveis normais de vários valores operacionais. Esses valores de linha de base, e desvios dessas linhas de base, podem fornecer pistas valiosas.	<ul style="list-style-type: none"> • Estabeleça linhas de base
Execute 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 os vistos ao usar o aplicativo cliente.	<ul style="list-style-type: none"> • "Monitore O PUT e obtenha desempenho"
Rever mensagens de auditoria	Revise as mensagens de auditoria para seguir 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.	<ul style="list-style-type: none"> • "Rever mensagens de auditoria"
Verifique os locais 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 storage.	<ul style="list-style-type: none"> • "Monitorar operações de verificação de objetos" • "Confirmar localizações de dados do objeto" • "Verifique a 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.	<ul style="list-style-type: none"> • "Colete arquivos de log e dados do sistema" • "Azione manualmente um pacote AutoSupport" • "Analise as métricas de suporte"

Crie uma linha do tempo de mudanças recentes

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

- As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.
- Uma linha do tempo de mudanças pode ajudá-lo 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, tais informações sobre o que mais estava acontecendo enquanto a mudança estava em andamento:

Hora da mudança	Tipo de alteração	Detalhes
<p>Por exemplo:</p> <ul style="list-style-type: none"> • Quando você iniciou a recuperação do nó? • Quando a atualização de software foi concluída? • Interrompeu o processo? 	<p>O que aconteceu? O que fez?</p>	<p>Documente todos os detalhes relevantes sobre a alteração. Por exemplo:</p> <ul style="list-style-type: none"> • Detalhes das alterações de rede. • Qual hotfix foi instalado. • Como as cargas de trabalho do cliente mudaram. <p>Certifique-se de observar se mais de uma mudança estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?</p>

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi recentemente instalado, expandido ou recuperado?
- O sistema foi atualizado recentemente? Foi aplicado um hotfix?
- Algum hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?
- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento mudou?
- Você alterou平衡adores de carga ou adicionou ou removeu um grupo de alta disponibilidade de nós de administrador ou nós de gateway?
- Foram iniciadas tarefas que podem demorar muito tempo a concluir? Os exemplos incluem:
 - Recuperação de um nó de storage com falha
 - Desativação do nó de storage
- Alguma alteração foi feita à autenticação do usuário, como adicionar um locatário ou alterar a configuração LDAP?
- A migração de dados está ocorrendo?
- Os serviços de plataforma foram recentemente ativados ou alterados?
- A conformidade foi ativada recentemente?
- Os pools de armazenamento em nuvem foram adicionados ou removidos?
- Alguma alteração foi feita na compactação ou criptografia de armazenamento?
- Houve alguma alteração na infra-estrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Alguma alteração foi feita em fontes NTP?
- Alguma alteração foi feita nas interfaces Grid, Admin ou Client Network?
- Alguma alteração de configuração foi feita no nó Arquivo?
- Alguma outra alteração foi feita ao sistema StorageGRID ou ao seu ambiente?

Estabeleça linhas de base

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

Propriedade	Valor	Como obter
Consumo médio de storage	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - dados do objeto, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar a quantidade de armazenamento consumida a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.
Consumo médio de metadados	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - metadados de objetos, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido diariamente 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 Performance > S3 operations ou Performance > Swift operations . Para ver as taxas de ingestão e recuperação e contagens de um site ou nó específico, selecione NÓS > site ou nó de armazenamento > objetos . Posicione o cursor sobre o gráfico de ingestão e recuperação para S3 ou Swift.
Falha nas operações S3/Swift	Operações	Selecione SUPPORT > Tools > Grid topology . Na guia Visão geral na seção operações da API, veja o valor de operações S3 - Falha ou operações rápidas - Falha.

Propriedade	Valor	Como obter
Taxa de avaliação ILM	Objetos/segundo	<p>Na página nós, selecione grid > ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para taxa de avaliação para o seu sistema.</p>
Taxa de digitalização ILM	Objetos/segundo	<p>Selecione NODES > grid > ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para taxa de digitalização para o seu sistema.</p>
Objetos enfileirados de operações do cliente	Objetos/segundo	<p>Selecione NODES > grid > ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de linha de base para objetos enfileirados (de operações do cliente) para o seu sistema.</p>
Latência média da consulta	Milissegundos	Selecione NODES > Storage Node > Objects . Na tabela consultas, exiba o valor da latência média.

Analizar dados

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

A análise é dependente de problemas, mas em geral:

- Localize pontos de falha e gargalos usando os alarmes.
- Reconstrua o histórico de problemas utilizando o histórico de alarmes e as tabelas.
- Use gráficos para encontrar anomalias e comparar a situação do problema com a operação normal.

Lista de verificação de informações de encaminhamento

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 de problemas.

	Item	Notas
	Declaração do problema	<p>Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, que horas ocorreu?</p> <p>Defina o problema</p>
	Avaliação de impactos	<p>Qual é a gravidade do problema? Qual é o impactos na aplicação cliente?</p> <ul style="list-style-type: none"> • O cliente foi conetado com sucesso antes? • O cliente pode obter, recuperar e excluir dados?
	ID do sistema StorageGRID	<p>Selecione MAINTENANCE > System > License. A ID do sistema StorageGRID é apresentada como parte da licença atual.</p>
	Versão do software	<p>Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione sobre para ver a versão do StorageGRID.</p>
	Personalização	<p>Resumir como o seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte:</p> <ul style="list-style-type: none"> • A grade usa compactação de storage, criptografia de storage ou conformidade? • O ILM faz objetos replicados ou codificados por apagamento? O ILM garante a redundância do site? As regras do ILM usam os comportamentos de ingestão equilibrada, rigorosa ou dupla confirmação?
	Ficheiros de registo e dados do sistema	<p>Recolha ficheiros de registo e dados do sistema para o seu sistema. Selecione SUPPORT > Tools > Logs.</p> <p>Você pode coletar logs para toda a grade ou para nós selecionados.</p> <p>Se você estiver coletando logs somente para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de storage em um local incluem o serviço ADC.)</p> <p>"Colete arquivos de log e dados do sistema"</p>
	Informações da linha de base	<p>Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento.</p> <p>Estabeleça linhas de base</p>

Item	Notas
Cronograma das mudanças recentes	<p>Crie uma linha do tempo que resume quaisquer alterações recentes ao sistema ou ao seu ambiente.</p> <p>Crie uma linha do tempo das mudanças recentes</p>
Histórico de esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, certifique-se de Registrar as etapas que você tomou e o resultado.

Solucionar problemas de objetos e storage

Confirmar localizações de dados do objeto

Dependendo do problema, você pode querer "[confirme onde os dados do objeto estão sendo armazenados](#)". Por exemplo, você pode querer verificar se a política ILM está funcionando como esperado e os dados do objeto estão sendo armazenados onde se pretende.

Antes de começar

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

Passos

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

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

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

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

source/testobject

Version ID (optional)

MEJGMkMyQzgtNEY5OC0xMUU3LTkzMELYtRDkyNTAwQkY5N0Mx

Look Up

4. Selecione **Procurar**.

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

- Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), o nome do objeto, o nome do contentor, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
- Para cópias de objetos replicadas, o local de storage atual de cada cópia.
- Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos de várias partes, uma lista de segmentos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os primeiros 100 segmentos são mostrados.
- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não são garantidos para persistir de liberação para liberação.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

Falhas no armazenamento de objetos (volume de storage)

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

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

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Para ver mais "[Detalhes sobre cada nó de storage](#)", siga estas etapas:

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **site > Storage Node > LDR > Storage > Overview > Main**.

The screenshot shows the Storage Node Overview page for LDR (DC1-S1). It includes sections for Storage State, Utilization, Replication, and Object Store Volumes, each with a table and a status bar.

Storage State

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors	
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors	
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors	

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

Verifique a integridade do objeto

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

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

O que é a verificação em segundo plano?

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

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

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



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

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

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

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

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

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

Se a verificação em segundo plano não puder substituir um objeto corrompido porque ele não consegue localizar outra cópia, o alerta **objetos perdidos** é acionado.

Altere a taxa de verificação em segundo plano

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

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você "[permissões de acesso específicas](#)" tem .

Sobre esta tarefa

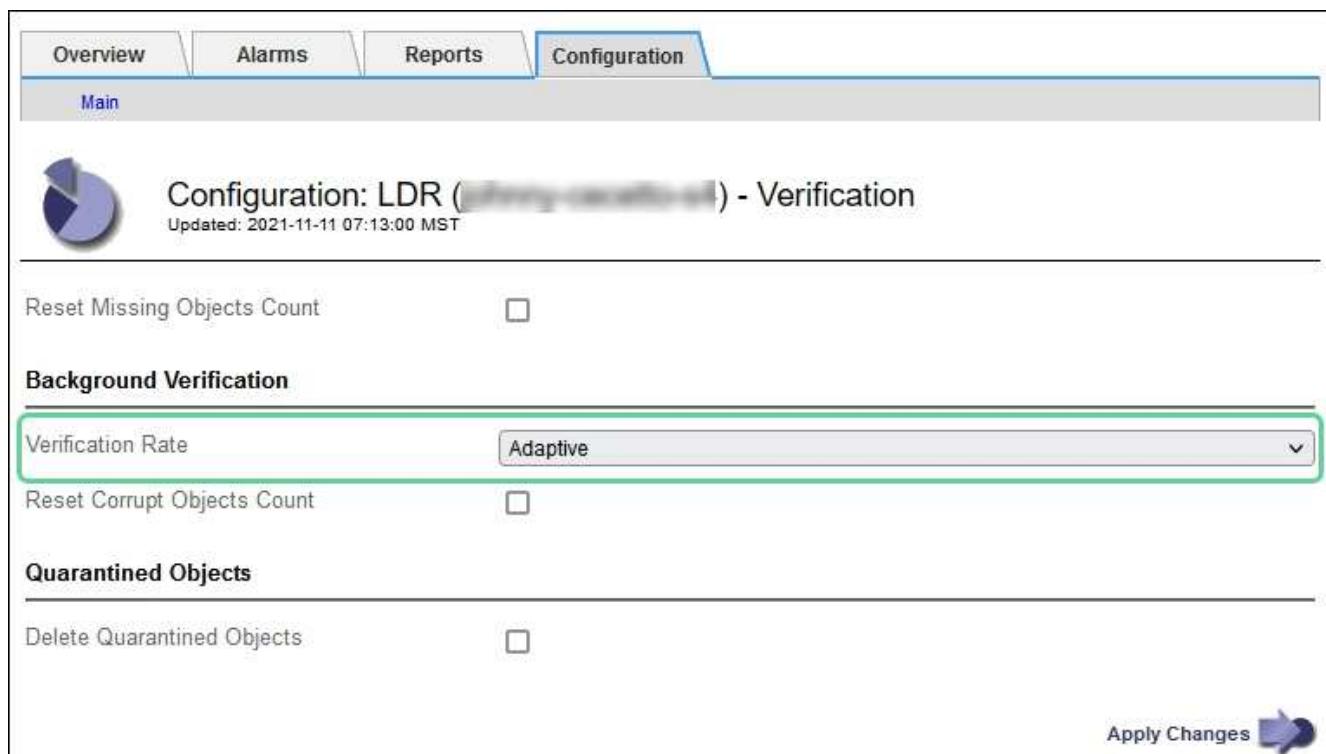
Você pode alterar a taxa de verificação para verificação em segundo plano em um nó de storage:

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

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

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Storage Node > LDR > Verificação**.
3. Selecione **Configuração > Principal**.
4. Aceda a **LDR > Verificação > Configuração > Principal**.
5. Em Verificação em segundo plano, selecione **taxa de verificação > alta ou taxa de verificação > adaptável**.



Configuration: LDR ([REDACTED]) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count

Background Verification

Verification Rate

Reset Corrupt Objects Count

Quarantined Objects

Delete Quarantined Objects

Apply Changes 



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

6. Clique em **aplicar alterações**.
7. Monitore os resultados da verificação em segundo plano para objetos replicados.
 - a. Vá para **NODES > Storage Node > Objects**.
 - b. Na seção Verificação, monitore os valores para **objetos corrompidos** e **objetos corrompidos não identificados**.

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

- Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar do sistema StorageGRID que satisfaça as políticas ativas de ILM.
 - Se o identificador de objeto não puder ser extraído (porque foi corrompido), a métrica **objetos corrompidos não identificados** é incrementada e o alerta **Objeto corrompido não identificado detetado** é acionado.
- c. Se forem encontrados dados de objeto replicados corrompidos, entre em Contato com o suporte técnico para determinar a causa raiz da corrupção.

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

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

- Selecione **SUPPORT > Tools > Grid topology**.
- Selecione **Storage Node > LDR > Erasure Coding**.
- Na tabela resultados da verificação, monitore o atributo fragmentos corrompidos detetados (ECCD).

9. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID, redefina a contagem de objetos corrompidos.

- Selecione **SUPPORT > Tools > Grid topology**.
- Selecione **Storage Node > LDR > Verificação > Configuração**.
- Selecione **Redefinir contagem de objetos corrompidos**.
- Clique em **aplicar alterações**.

10. Se você estiver confiante de que objetos em quarentena não são necessários, você pode excluí-los.



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

- Selecione **SUPPORT > Tools > Grid topology**.
- Selecione **Storage Node > LDR > Verificação > Configuração**.
- Selecione **Excluir objetos em quarentena**.
- Selecione **aplicar alterações**.

O que é verificação de existência de objeto?

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

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

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

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

Executar verificação de existência de objeto

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

Antes de começar

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

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

Sobre esta tarefa

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

Passos

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

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

Você pode pesquisar por nome do nó ou site.

Não é possível selecionar nós que não estão 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 do trabalho.

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

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

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

8. Selecione **continuar**.

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

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

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



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

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

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

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

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job **Job history**

Status: Accepted	Consistency control: All
Job ID: 2334602652907829302	Start time: 2021-11-10 14:43:02 MST
Missing object copies detected: 0	Elapsed time: —
Progress: 0%	Estimated time to completion: —

Pause **Cancel**

Volumes **Details**

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Após a conclusão do trabalho, execute quaisquer ações adicionais necessárias:

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

Este procedimento é semelhante ao de "[investigando objetos perdidos](#)", embora para cópias de objetos que você pesquise em LLST vez OLST de .

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

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

perdidas.

- a. Selecione **MAINTENANCE > Object existence check > Job history**.
- b. Determine quais trabalhos estão prontos para serem executados novamente:
 - i. Olhe para a coluna **hora de fim** para determinar quais trabalhos foram executados há mais de três semanas.
 - ii. Para esses trabalhos, examine a coluna de controle de consistência para sites fortes ou globais.
- c. Selecione a caixa de verificação para cada trabalho que pretende executar novamente e, em seguida, selecione **Reexecutar**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job		Job history		Search by Job ID/ node name/ consistency control/ start time				Displaying 4 results	
<input type="button" value="Delete"/>	<input type="button" value="Rerun"/>								
	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time		
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:06 MST (3 weeks ago)		2021-11-10 14:43:06 MST (3 weeks ago)	
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST (17 minutes ago)		2021-11-10 14:42:10 MST (17 minutes ago)	

- d. No assistente de reexecução de trabalhos, reveja os nós e volumes selecionados e a consistência.
- e. Quando estiver pronto para executar novamente os trabalhos, selecione **Reexecutar**.

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

Depois de terminar

Se ainda tiver preocupações sobre a integridade dos dados, aceda a **SUPPORT > Tools > Grid topology > site > Storage Node > LDR > Verification > Configuration > Main** e aumente a taxa de verificação em segundo plano. A verificação em segundo plano verifica a exatidão de todos os dados de objetos armazenados e repara quaisquer problemas que encontrar. Encontrar e reparar possíveis problemas o mais rápido possível reduz o risco de perda de dados.

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

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

Antes de começar

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

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

Passos

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

- a. Introduza `ssh admin@primary_Admin_Node_IP`
- b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- c. Digite o seguinte comando para mudar para root: `su -`
- d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

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

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

Opção	Destino
Nós locais (padrão)	<code>/var/local/log/localaudit.log</code>
Nós de administração/nós locais	<ul style="list-style-type: none">• Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code>• Todos os nós: O <code>/var/local/log/localaudit.log</code> arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

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

Para saber mais, ["Selecionar destinos de informações de auditoria"](#) consulte .

- f. Identifique quais locatários estão usando objetos maiores que 5 GiB.
 - i. Introduza `zgrep SPUT * | egrep "CSIZ\ (UI64\) : ([5-9]\|[1-9]\ [0-9]\+)\ [0-9]\{9\}"`

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

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

Exemplo de resultados de log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"060X85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(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):PUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

- Aceda a **SUPPORT > Tools > Logs**. Colete logs de aplicativos para o nó de armazenamento no alerta. Especifique 15 minutos antes e depois do alerta.
- Extraia o arquivo e vá `broadcast.log` para :

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

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

Exemplo broadcast.log

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

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

Solucionar problemas de dados de objetos perdidos e ausentes

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

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

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

Se esta recuperação for bem-sucedida, o sistema StorageGRID substitui a cópia em falta do objeto. Caso contrário, o alerta **objetos perdidos** é acionado, da seguinte forma:

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

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

No caso de perda de dados de objetos sem cópias, não há solução de recuperação. No entanto, você deve redefinir o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos. ["Repor contagens de objetos perdidas e em falta"](#) Consulte .

Investigue objetos perdidos

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

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#) tem .

- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

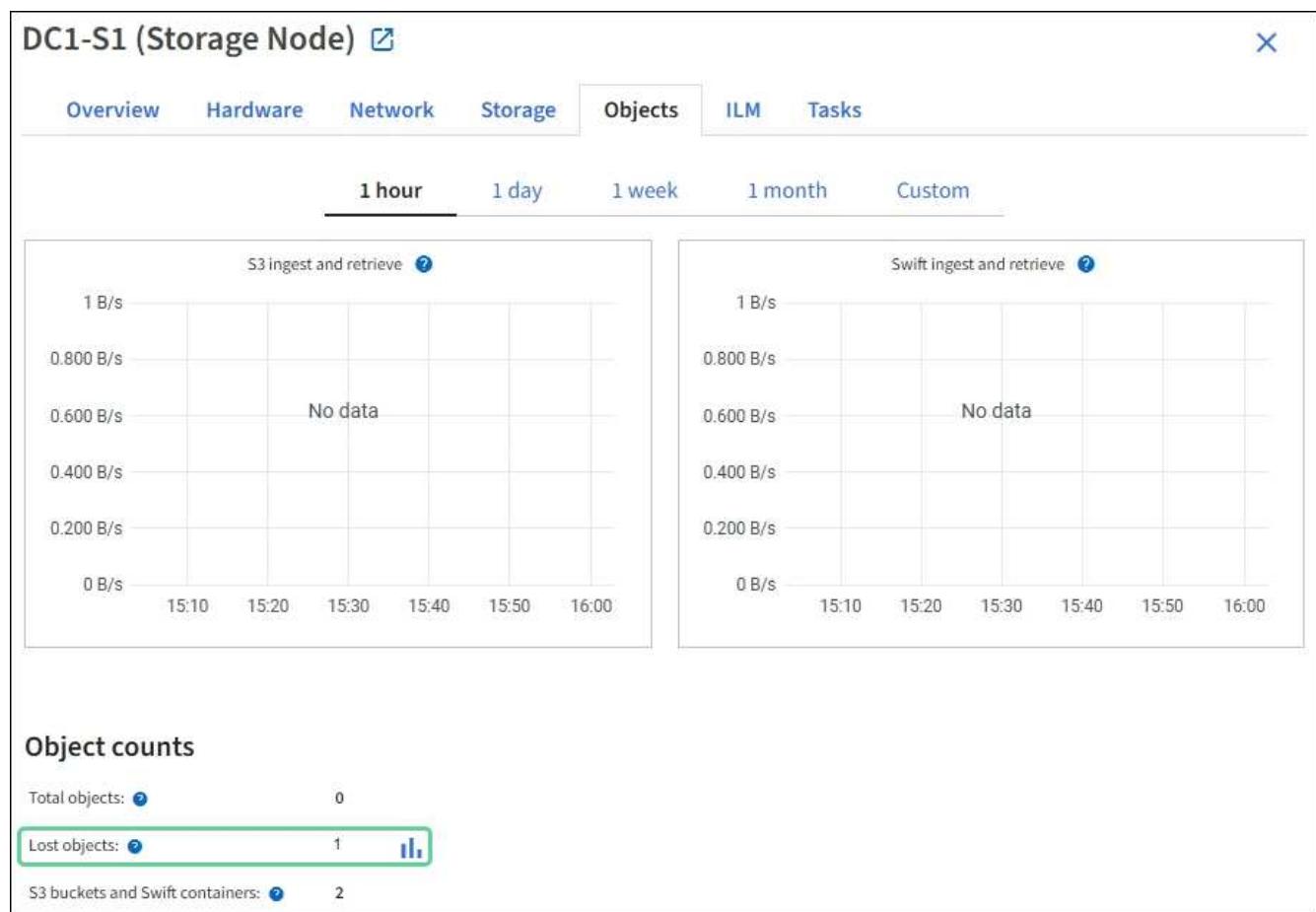
O alerta **objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

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

Passos

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

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



4. A partir de um nó Admin, "[acesse o log de auditoria](#)" para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **objetos perdidos**:
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

- iii. Digite o seguinte comando para mudar para root: `su -`
- iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conectado como root, o prompt mudará de `$` para `#`.
- b. Mude para o diretório onde os logs de auditoria estão localizados.

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

Opção	Destino
Nós locais (padrão)	<code>/var/local/log/localaudit.log</code>
Nós de administração/nós locais	<ul style="list-style-type: none"> • Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code> • Todos os nós: O <code>/var/local/log/localaudit.log</code> arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

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

Para saber mais, "["Selecionar destinos de informações de auditoria"](#) consulte .

- c. Use grep para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`
- d. Observe o valor UUID incluído na mensagem.

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

- 5. Use o `ObjectByUUID` comando para encontrar o objeto pelo seu identificador (UUID) e, em seguida, determinar se os dados estão em risco.
 - a. Use SSH para fazer login em qualquer nó de armazenamento. Em seguida, aceda à consola LDR introduzindo "telnet 0 1402".
 - b. Introduza: `/proc/OBRP/ObjectByUUID UUID_value`

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

```

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

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\ (Locations\)": \[
        \{
            "Location Type": "CLDI\ (Location online\)",
            "NOID\ (Node ID\)": "12448208",
            "VOLI\ (Volume ID\)": "3222345473",
            "Object File Path":
            "/var/local/rangedb/1/p/17/11/00rH0%DkRt78I1a\#3udu",
            "LTIM\ (Location timestamp\)": "2020-02-

```

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

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

```

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

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

```

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

Metadados	Conclusão
Nenhum objeto encontrado ("ERRO": "")	<p>Se o objeto não for encontrado, a mensagem "ERROR": é retornada.</p> <p>Se o objeto não for encontrado, você pode redefinir a contagem de objetos perdidos para limpar o alerta. A falta de um objeto indica que o objeto foi intencionalmente excluído.</p>
Localizações > 0	<p>Se houver locais listados na saída, o alerta objetos perdidos pode ser um falso positivo.</p> <p>Confirme se os objetos existem. Use o ID do nó e o filepath listados na saída para confirmar se o arquivo de objeto está no local listado.</p> <p>(O procedimento para "procurar objetos potencialmente perdidos" explica como usar o ID do nó para encontrar o nó de armazenamento correto.)</p> <p>Se os objetos existirem, você pode redefinir a contagem de objetos perdidos para limpar o alerta.</p>
Localização: 0	<p>Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar "procure e restaure o objeto" para si mesmo, ou você pode entrar em Contato com o suporte técnico.</p> <p>O suporte técnico pode pedir-lhe para determinar se existe um procedimento de recuperação de armazenamento em curso. Consulte as informações sobre "Restaurando dados de objetos usando o Grid Manager" e "restaurar dados de objeto para um volume de armazenamento".</p>

Procure e restaure objetos potencialmente perdidos

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

Antes de começar

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

Sobre esta tarefa

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



Contacte o suporte técnico para obter assistência com este procedimento.

Passos

1. A partir de um nó Admin, procure os logs de auditoria para possíveis localizações de objetos:

a. Faça login no nó da grade:

- i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
- ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- iii. Digite o seguinte comando para mudar para root: `su -`
- iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conectado como root, o prompt mudará de `$` para `#`.

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

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

Opção	Destino
Nós locais (padrão)	<code>/var/local/log/localaudit.log</code>
Nós de administração/nós locais	<ul style="list-style-type: none">• Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code>• Todos os nós: O <code>/var/local/log/localaudit.log</code> arquivo está normalmente vazio ou ausente neste modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

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

Para saber mais, "["Selecionar destinos de informações de auditoria"](#) consulte .

c. Use grep para extrair o "auditar mensagens associadas ao objeto potencialmente perdido" e enviá-los para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

Por exemplo:

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

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

Por exemplo:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

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

```
[AUDT: [NOID (UI32) :12448208] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) :"926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP (FC32) :CLDI]
[PCLD (CSTR) :"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :15815351
34379225]
[ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CLSM] [ATID (UI64) :70
86871083190743409]
```

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

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

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

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

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

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

- a. Faça login no nó da grade:

- i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
- ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- iii. Digite o seguinte comando para mudar para root: `su -`
- iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

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

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

Por exemplo, digite:

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



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

- Se o caminho do objeto não for encontrado, o objeto é perdido e não pode ser restaurado usando este procedimento. Entre em Contato com o suporte técnico.

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

3. Se o caminho do objeto foi encontrado, tente restaurar o objeto para StorageGRID:

- No mesmo nó de storage, altere a propriedade do arquivo de objeto para que ele possa ser gerenciado pelo StorageGRID. Introduza: `chown ldr-user:bycast 'file_path_of_object'`
- Use SSH para fazer login em qualquer nó de armazenamento. Em seguida, acceda à consola LDR introduzindo "telnet 0 1402".
- Introduza: `cd /proc/STOR`
- Introduza: `Object_Found 'file_path_of_object'`

Por exemplo, digite:

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

A emissão do `Object_Found` comando notifica a grade da localização do objeto. Ele também aciona as políticas ILM ativas, que fazem cópias adicionais conforme especificado em cada política.



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

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

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

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78I1a#3udu'
```

Avance para o passo seguinte.

4. Se o objeto foi restaurado com sucesso para o StorageGRID, verifique se novos locais foram criados.

- Introduza: `cd /proc/OBRP`
- Introduza: `ObjectByUUID UUID_value`

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

```

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

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1dff7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\ (Locations)": \[
        \{
            "Location Type": "CLDI\ (Location online\)",
            "NOID\ (Node ID)": "12448208",
            "VOLI\ (Volume ID)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\ (Location timestamp)": "2020-02-12T19:36:17.880569"
        },

```

```

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

```

- a. Saia da consola LDR. Introduza: `exit`
5. Em um nó Admin, pesquise os logs de auditoria para a mensagem de auditoria ORLM para este objeto para confirmar que o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme necessário.
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conectado como root, o prompt mudará de `$` para `#`.
 - b. Mude para o diretório onde os logs de auditoria estão localizados. [subetapa 1. b](#) Consulte a .
 - c. Use grep para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

Por exemplo:

```

Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt

```

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

Por exemplo:

```

Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt

```

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

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

- a. Localize o campo LOCS na mensagem de auditoria.

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

6. ["Redefina as contagens de objetos perdidas e ausentes"](#) No Gerenciador de Grade.

Rapor contagens de objetos perdidas e em falta

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

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você "[permissões de acesso específicas](#)" tem .

Sobre esta tarefa

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

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

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

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Site > Storage Node > LDR > armazenamento de dados > Configuração** para o nó de armazenamento que tem o alerta **objetos perdidos** ou o alarme **PERDIDO**.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **aplicar alterações**.

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

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

- a. Selecione **Site > Storage Node > LDR > Codificação de apagamento > Configuração**.
- b. Selecione **Redefinir leituras de contagem de falhas** e **Redefinir cópias corrompidas detetadas contagem**.
- c. Clique em **aplicar alterações**.
- d. Selecione **Site > Storage Node > LDR > Verificação > Configuração**.
- e. Selecione **Redefinir contagem de objetos ausentes** e **Redefinir contagem de objetos corrompidos**.
- f. Se você tiver certeza de que objetos em quarentena não são necessários, selecione **Excluir objetos em quarentena**.

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

g. Clique em **aplicar alterações**.

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

Solucionar problemas do alerta de armazenamento de dados de objetos baixos

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Nesta condição:

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

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

Passos

1. Selecione **ALERTAS > atual**.

A página Alertas é exibida.

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



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

3. Revise os detalhes na caixa de diálogo e observe o seguinte:

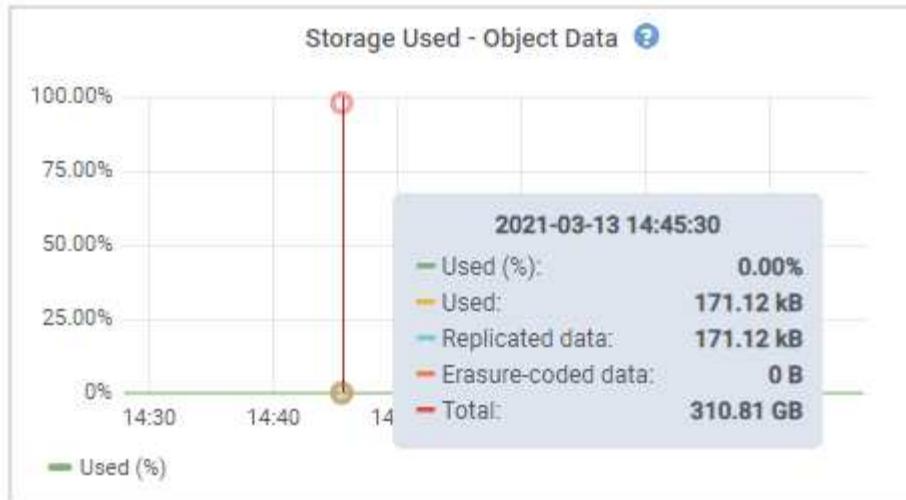
- Tempo acionado
- O nome do site e do nó
- Os valores atuais das métricas para este alerta

4. Selecione **NÓS > Storage Node ou Site > Storage**.

5. Posicione o cursor sobre o gráfico armazenamento usado - dados do objeto.

São apresentados os seguintes valores:

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



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

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

7. Assim que possível, ["adicionar capacidade de armazenamento"](#) para a sua grade.

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



Para obter mais informações, ["Gerencie nós de storage completos"](#) consulte .

Informações relacionadas

["Resolução de problemas do alarme de estado de armazenamento \(SSTS\) \(legado\)"](#)

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

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

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

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

- Seu sistema está próximo da capacidade e não poderá aceitar novos dados se forem aplicadas marcas de

água otimizadas. Neste caso, o StorageGRID não alterará as configurações de marca d'água.

- Você definiu anteriormente qualquer uma das marcas d'água do volume de armazenamento para um valor personalizado. O StorageGRID não substituirá as configurações personalizadas de marca d'água com valores otimizados. No entanto, o StorageGRID pode acionar o alerta de substituição de marca d'água **baixa somente leitura** se o valor personalizado para a marca d'água de volume de armazenamento Soft somente leitura for muito pequeno.

Entenda o alerta

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

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

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

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

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

Resolva o alerta

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

Antes de começar

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

Sobre esta tarefa

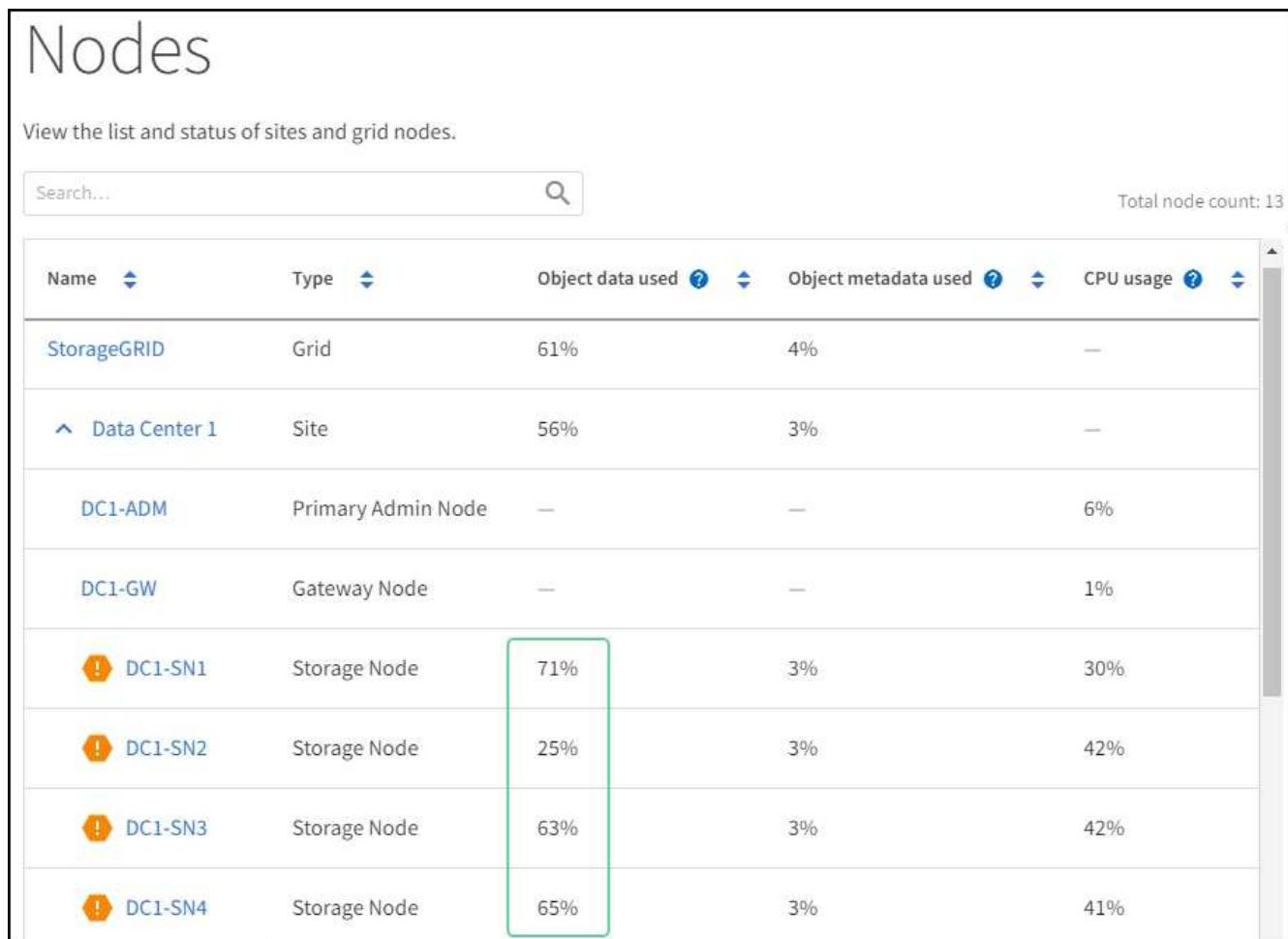
Você pode resolver o alerta * baixa substituição de marca d'água somente leitura * atualizando as

configurações personalizadas de marca d'água para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem próximos do cheio ou se você tiver requisitos especiais de ILM, primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados de objeto para toda a grade

Passos

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



Nodes					
View the list and status of sites and grid nodes.					
Search...		Object data used		Object metadata used	
Name	Type	Object data used	Object metadata used	CPU usage	
StorageGRID	Grid	61%	4%	—	
▲ Data Center 1	Site	56%	3%	—	
DC1-ADM	Primary Admin Node	—	—	6%	
DC1-GW	Gateway Node	—	—	1%	
⚠ DC1-SN1	Storage Node	71%	3%	30%	
⚠ DC1-SN2	Storage Node	25%	3%	42%	
⚠ DC1-SN3	Storage Node	63%	3%	42%	
⚠ DC1-SN4	Storage Node	65%	3%	41%	

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

Ver marcas de água de armazenamento otimizadas

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

Passos

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

```
storagegrid_storage_volume_minimum_optimized_soft_READONLY_watermark
```

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

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

```
storagegrid_storage_volume_maximum_optimized_soft_READONLY_watermark
```

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

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

determine se você pode usar marcas de água otimizadas

Passos

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

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

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



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

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

Passos

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

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

Solucionar o problema do alarme de Status de armazenamento (SSTS)

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

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você "[permissões de acesso específicas](#)" tem .

Sobre esta tarefa

O alarme SSTS (Storage Status) é acionado no nível de aviso quando a quantidade de espaço livre em cada volume em um nó de armazenamento cai abaixo do valor do volume de armazenamento Soft Read Only Watermark (**CONFIGURATION > System > Storage options**).



Storage Options Overview

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

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

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

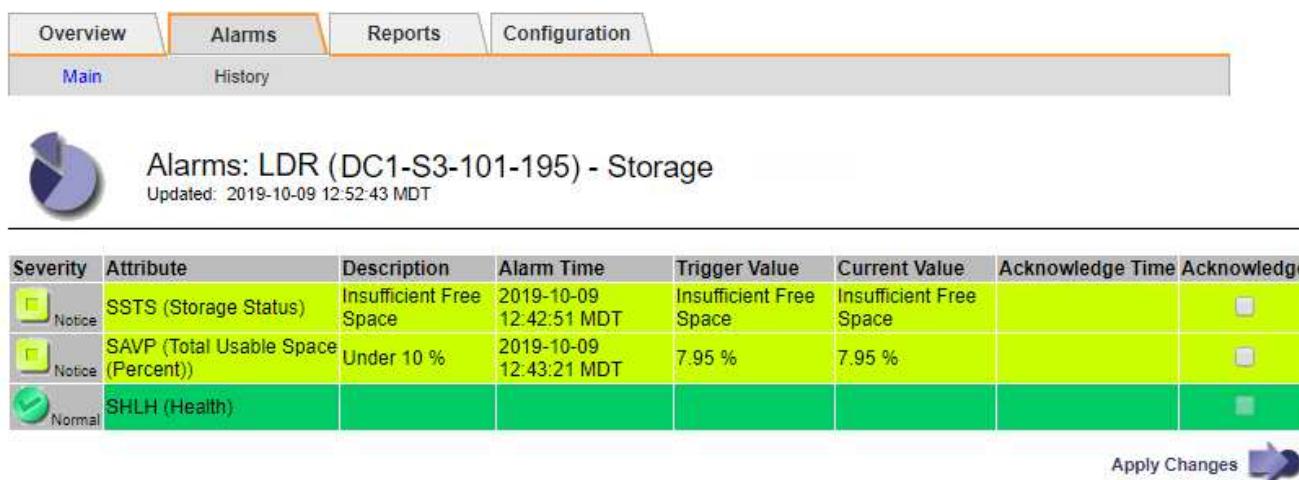
Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. O alarme SSTS é acionado se menos de 10 GB de espaço utilizável permanecer em cada volume de armazenamento no nó de armazenamento. Se algum dos volumes tiver 10 GB ou mais de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

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

Passos

1. Selecione **SUPPORT > Alarmes (legacy) > Current Alarms**.
2. Na coluna Serviço, selecione o data center, o nó e o serviço associados ao alarme SSTS.

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



Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input checked="" type="checkbox"/>

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



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

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



Overview: LDR (DC1-S1-101-193) - Storage

Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:

Online



Storage State - Current:

Read-only



Storage Status:

Insufficient Free Space



Utilization

Total Space:

164 GB



Total Usable Space:

19.6 GB



Total Usable Space (Percent):

11.937 %



Total Data:

139 GB



Total Data (Percent):

84.567 %



Replication

Block Reads:

0



Block Writes:

2,279,881



Objects Retrieved:

0



Objects Committed:

88,882



Objects Deleted:

16



Delete Service State:

Enabled



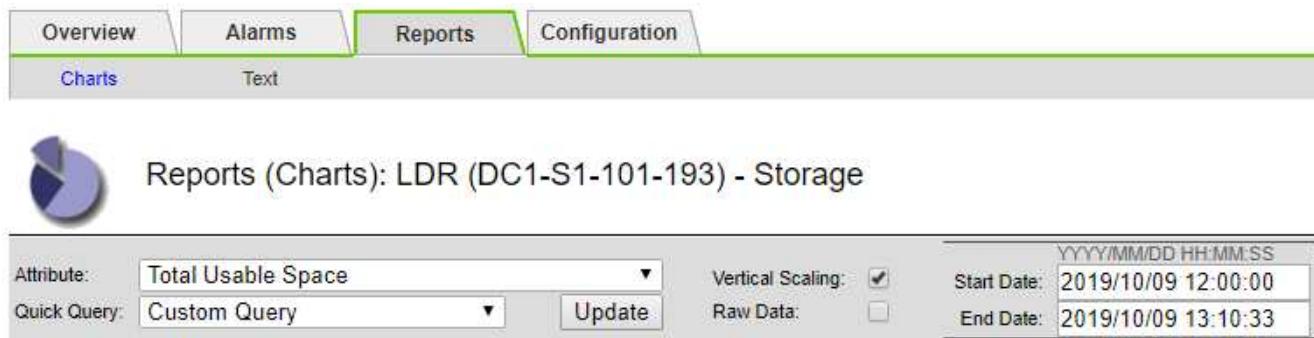
Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	46.2 GB	0 B	84.486 %	No Errors
0001	54.7 GB	8.32 GB	46.3 GB	0 B	84.644 %	No Errors
0002	54.7 GB	8.36 GB	46.3 GB	0 B	84.57 %	No Errors

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

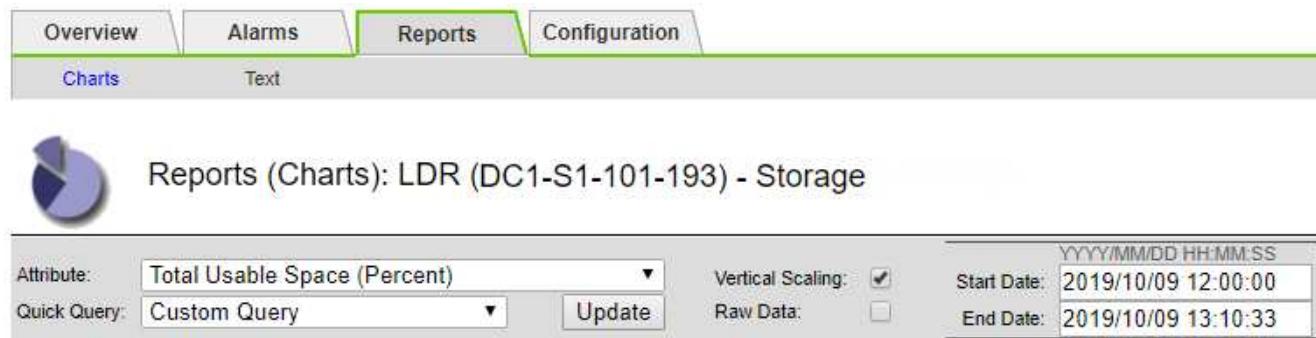
4. Para entender como o armazenamento foi usado ao longo do tempo, selecione a guia **relatórios** e plote o espaço utilizável total nas últimas horas.

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



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

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



6. Conforme necessário, "adicionar capacidade de armazenamento".

Consulte também "[Gerencie nós de storage completos](#)".

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

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

Sobre esta tarefa

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

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

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

Para obter informações adicionais, consulte o "["Solucionar problemas de serviços de plataforma"](#)". Talvez seja necessário "[Acesse o locatário do Gerenciador do Locatário](#)" depurar um erro de serviço de plataforma.

Passos

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

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

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

Solucionar problemas de metadados

Você pode executar várias tarefas para ajudar a determinar a origem dos problemas de metadados.

Alerta baixo de armazenamento de metadados

Se o alerta **armazenamento de metadados baixo** for acionado, você deverá adicionar novos nós de armazenamento.

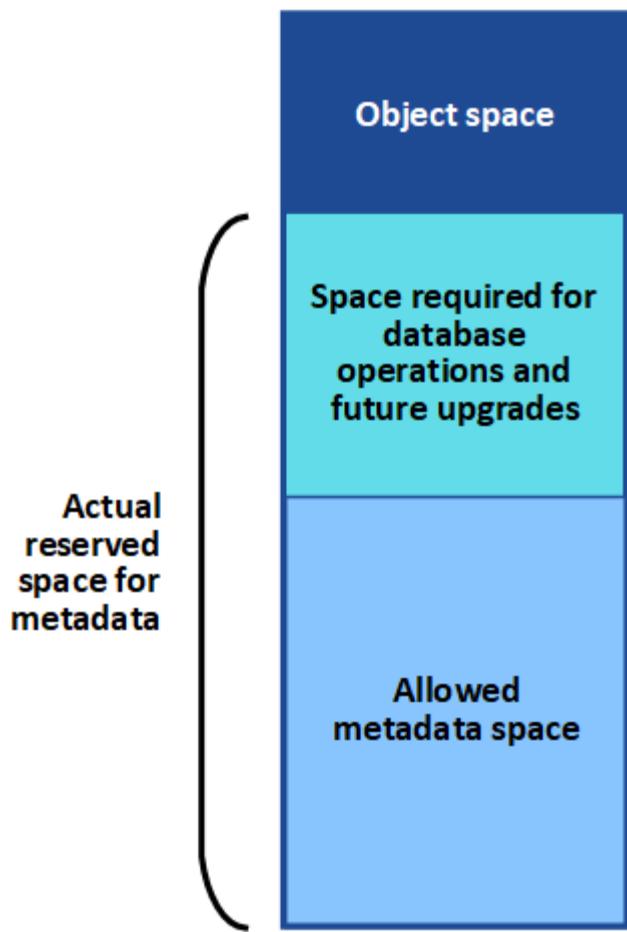
Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".

Sobre esta tarefa

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

Volume 0



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

Você pode ["Monitore a capacidade dos metadados de objetos para cada nó de storage"](#) ajudá-lo a antecipar erros e corrigi-los antes que eles ocorram.

O StorageGRID usa a seguinte métrica Prometheus para medir o quanto cheio é o espaço permitido de metadados:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

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

- **Minor:** Metadados de objetos estão usando 70% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de storage o mais rápido possível.
- **Major:** Metadados de objetos estão usando 90% ou mais do espaço permitido de metadados. Você deve adicionar novos nós de storage imediatamente.



Quando os metadados de objetos estão usando 90% ou mais do espaço permitido de metadados, um aviso aparece no painel. Se esse aviso for exibido, você deverá adicionar novos nós de storage imediatamente. Você nunca deve permitir que os metadados de objetos usem mais de 100% do espaço permitido.

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

No exemplo a seguir, metadados de objetos estão usando mais de 100% do espaço permitido de metadados. Esta é uma situação crítica, o que resultará em erros e operações ineficientes do banco de dados.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

Se o tamanho do volume 0 for menor do que a opção de armazenamento de espaço reservado de metadados (por exemplo, em um ambiente não-produção), o cálculo do alerta **armazenamento de metadados baixo** pode 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 exibir.
3. Reveja os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **armazenamento de metadados baixo** tiver sido acionado, execute uma expansão para adicionar nós de armazenamento imediatamente.



Como o StorageGRID mantém cópias completas de todos os metadados de objetos em cada local, a capacidade de metadados de toda a grade é limitada pela capacidade de metadados do menor local. Se você precisar adicionar capacidade de metadados a um local, também deverá ["expanda quaisquer outros sites"](#) pelo mesmo número de nós de storage.

Após a expansão, o StorageGRID redistribui os metadados de objetos existentes para os novos nós, o que aumenta a capacidade geral de metadados da grade. Nenhuma ação do usuário é necessária. O alerta **armazenamento de metadados baixo** é apagado.

Serviços: Status - alarme Cassandra (SVST)

O alarme Serviços: Status - Cassandra (SVST) indica que você pode precisar reconstruir o banco de dados Cassandra para um nó de armazenamento. O Cassandra é usado como o armazenamento de metadados do StorageGRID.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você "[permissões de acesso específicas](#)" tem .
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Se o Cassandra for interrompido por mais de 15 dias (por exemplo, o nó de armazenamento está desligado), o Cassandra não será iniciado quando o nó for colocado novamente on-line. Você deve reconstruir o banco de dados Cassandra para o serviço DDS afetado.

Você pode "[execute o diagnóstico](#)" obter informações adicionais sobre o estado atual da sua grade.



Se dois ou mais serviços de banco de dados do Cassandra estiverem inativos por mais de 15 dias, entre em Contato com o suporte técnico e não prossiga com as etapas abaixo.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Site > Storage Node > SSM > Serviços > Alarmes > Principal** para exibir alarmes.

Este exemplo mostra que o alarme SVST foi acionado.

The screenshot shows the 'Alarms' tab selected in the SSM interface. The main content area displays the following information:

Alarms: SSM (DC1-S3) - Services
Updated: 2014-08-14 16:29:36 PDT

Severity Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:26 PDT	Not Running	Not Running		<input type="checkbox"/>

A página principal dos Serviços de SSM também indica que o Cassandra não está em execução.

3. Tente reiniciar o Cassandra a partir do nó de armazenamento:
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conectado como root, o prompt mudará de `$` para `#`.
 - b. Introduza: `/etc/init.d/cassandra status`
 - c. Se o Cassandra não estiver em execução, reinicie-o: `/etc/init.d/cassandra restart`
4. Se o Cassandra não reiniciar, determine quanto tempo o Cassandra esteve inativo. Se o Cassandra estiver inativo por mais de 15 dias, você deverá reconstruir o banco de dados do Cassandra.



Se dois ou mais serviços de banco de dados do Cassandra estiverem inoperantes, entre em Contato com o suporte técnico e não prossiga com as etapas abaixo.

Você pode determinar por quanto tempo o Cassandra ficou para baixo, traçando-o ou revisando o arquivo `servermanager.log`.

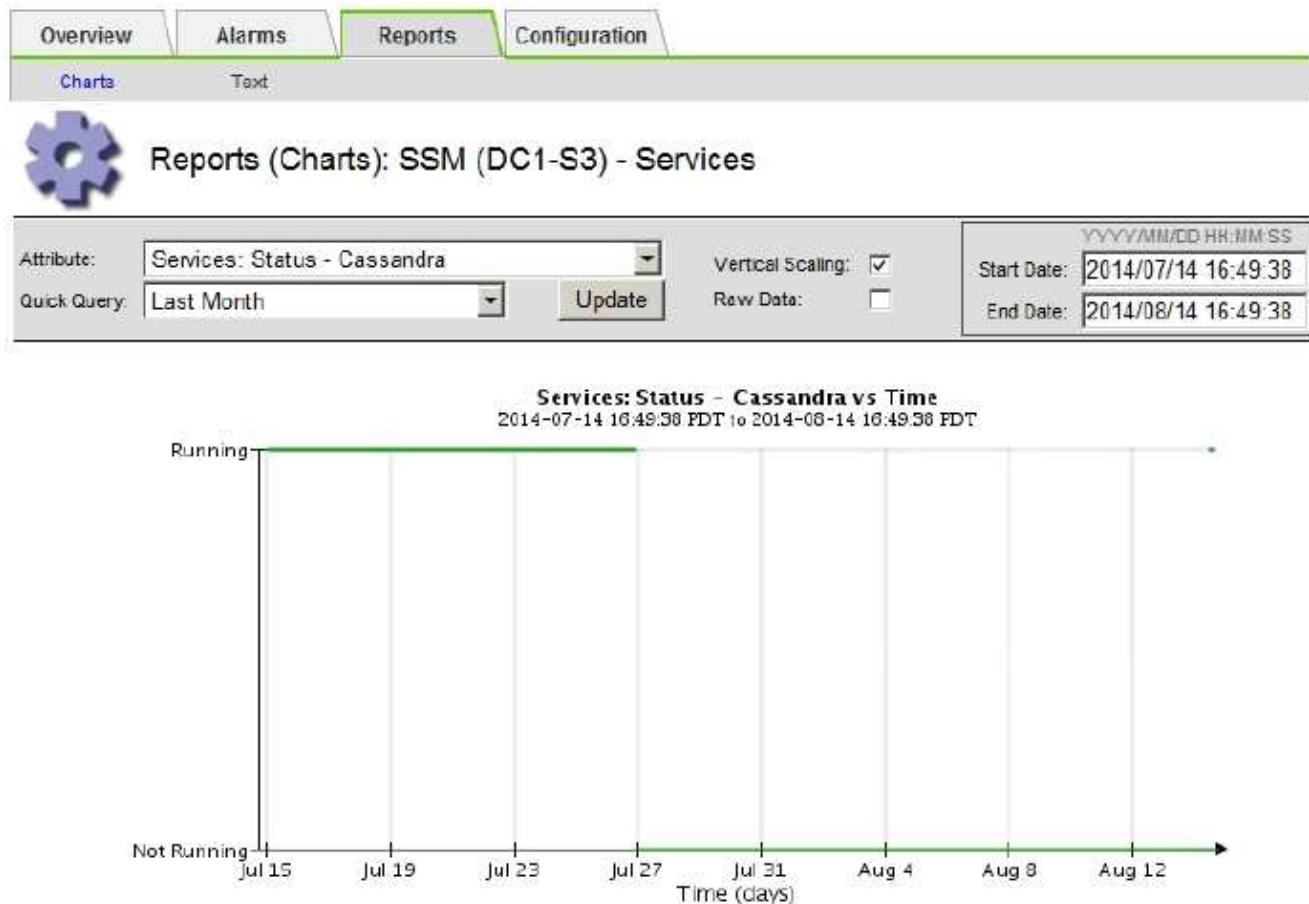
5. Para traçar o gráfico Cassandra:
 - a. Selecione **SUPPORT > Tools > Grid topology**. Em seguida, selecione **Site > Storage Node > SSM > Serviços > relatórios > gráficos**.
 - b. Selecione **Atributo > Serviço: Status - Cassandra**.
 - c. Para **Data de Início**, insira uma data que seja pelo menos 16 dias antes da data atual. Para **Data de**

fim, insira a data atual.

d. Clique em **Atualizar**.

e. Se o gráfico mostrar que o Cassandra está inativo por mais de 15 dias, reconstrua o banco de dados do Cassandra.

O exemplo de gráfico a seguir mostra que o Cassandra esteve inativo por pelo menos 17 dias.



6. Para analisar o arquivo servermanager.log no nó de storage:

a. Faça login no nó da grade:

- i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
- ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- iii. Digite o seguinte comando para mudar para root: `su -`
- iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conectado como root, o prompt mudará de `$` para `#`.

b. Introduza: `cat /var/local/log/servermanager.log`

O conteúdo do arquivo servermanager.log é exibido.

Se o Cassandra estiver inativo por mais de 15 dias, a seguinte mensagem é exibida no arquivo servermanager.log:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. Certifique-se de que o carimbo de data/hora desta mensagem é o momento em que você tentou reiniciar o Cassandra conforme instruído na etapa [Reinic peace o Cassandra a partir do nó de storage](#).

Pode haver mais de uma entrada para Cassandra; você deve localizar a entrada mais recente.

- b. Se o Cassandra estiver inativo por mais de 15 dias, você deverá reconstruir o banco de dados do Cassandra.

Para obter instruções, ["Recupere o nó de storage abaixo mais de 15 dias"](#) consulte .

- c. Entre em Contato com o suporte técnico se os alarmes não forem claros depois que o Cassandra for reconstruído.

Erros de memória sem Cassandra (alarme SMTT)

Um alarme de Eventos totais (SMTT) é acionado quando o banco de dados Cassandra tem um erro de memória fora. Se este erro ocorrer, contacte o suporte técnico para resolver o problema.

Sobre esta tarefa

Se ocorrer um erro de falta de memória para o banco de dados do Cassandra, um despejo de heap é criado, um alarme de Eventos totais (SMTT) é acionado e a contagem de erros de memória do Cassandra é incrementada por um.

Passos

1. Veja o evento:

- a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Expanda o site e selecione **grid_node**.
 - c. Selecione **SSM** e depois **Eventos > Configuração**.

2. Verifique se a contagem de erros de memória do Cassandra Heap é 1 ou superior.

Você pode ["execute o diagnóstico"](#) obter informações adicionais sobre o estado atual da sua grade.

3. Efetue login no nó selecionado como "admin" usando SSH e alterne para o usuário root local.
4. Vá para `/var/local/core/`, compacte o `Cassandra.hprof` arquivo e envie-o para o suporte técnico.
5. Faça um backup do `Cassandra.hprof` arquivo e exclua-o do `/var/local/core/` directory.

Este arquivo pode ter até 24 GB, então você deve removê-lo para liberar espaço.

6. Depois que o problema for resolvido, marque a caixa de seleção **Redefinir** para a contagem de erros de memória de saída do Cassandra. Em seguida, selecione **aplicar alterações**.



Para redefinir contagens de eventos, você deve ter a permissão de configuração de página de topologia de Grade.

Solucionar erros de certificado

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

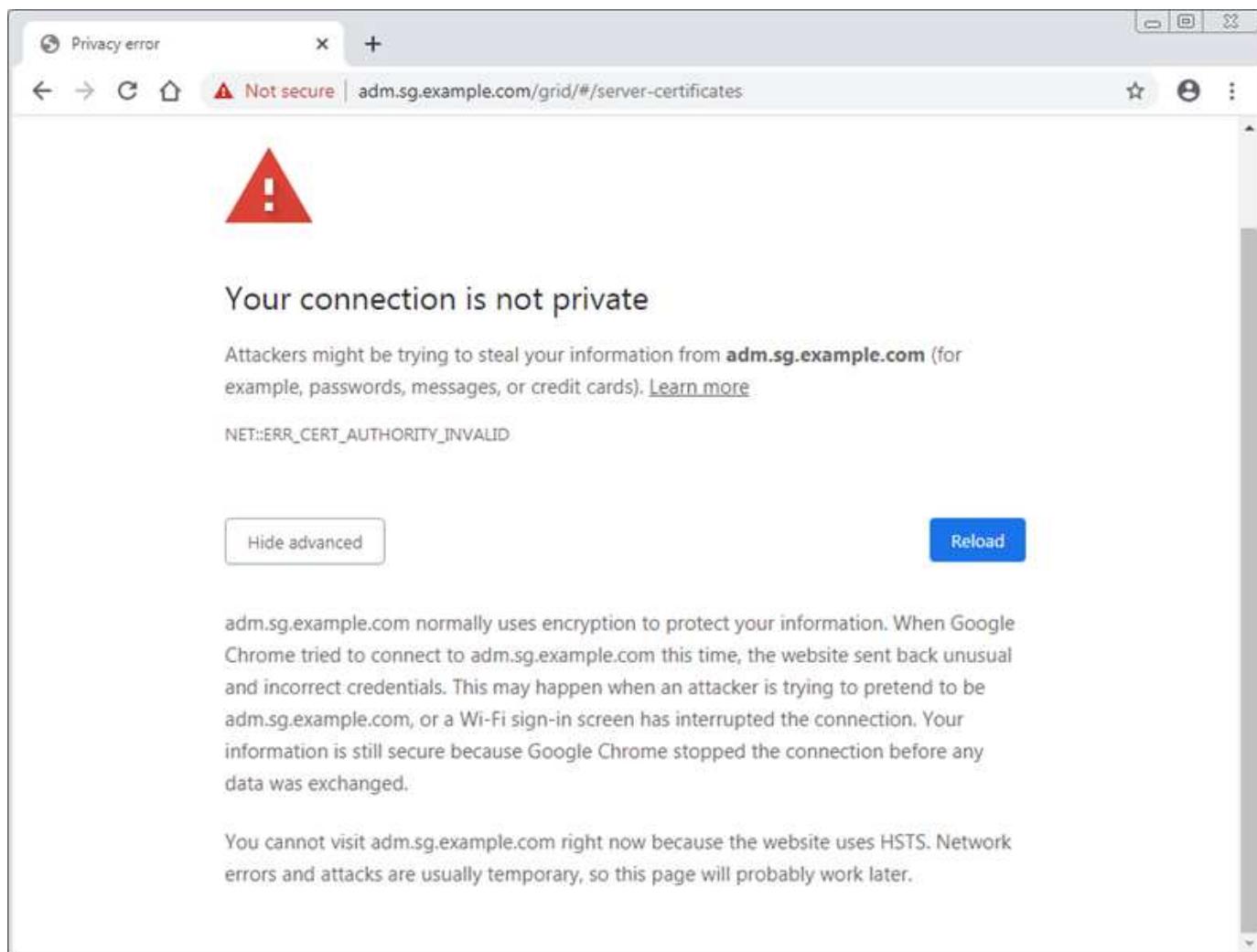
Sobre esta tarefa

Os erros de certificado podem causar problemas quando você tenta se conectar ao StorageGRID usando o Gerenciador de Grade, a API de Gerenciamento de Grade, o Gerenciador de Locatário ou a API de Gerenciamento de Locatário. Erros de certificado também podem ocorrer quando você tenta se conectar com um cliente S3 ou Swift ou ferramenta de monitoramento externa.

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

- O 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 de interface de gerenciamento personalizado expirou:



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Management Interface** é acionado quando o certificado do servidor está prestes a expirar.

Quando você estiver usando certificados de cliente para integração externa do Prometheus, erros de certificado podem ser causados pelo certificado de 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 **CONFIGURATION > Security > Certificates** e, em seguida "[selecione a guia certificado apropriado](#)", .

1. Verifique o período de validade do certificado. Alguns navegadores web e clientes S3 ou Swift não aceitam certificados com um período de validade superior a 398 dias.
2. Se o certificado tiver expirado ou expirar em breve, carregue ou gere um novo certificado.
 - Para obter um certificado de servidor, consulte as etapas "[Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário](#)" do .
 - Para obter um certificado de cliente, consulte as etapas "[configurando um certificado de cliente](#)" do .
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 a SAN corresponda ao endereço IP ou ao 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. Insira o endereço IP do nó Admin em vez do nome de domínio para ignorar o erro de conexão e acessar o Gerenciador de Grade.
 - ii. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida "[selecione a guia certificado apropriado](#)", instale um novo certificado personalizado ou continue com o certificado padrão.
 - iii. Nas instruções de administração do StorageGRID, consulte as etapas "[Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário](#)" do .

Solucionar problemas de nó de administração e interface do usuário

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

Erros de início de sessão

Se ocorrer um erro ao iniciar sessão num nó de administração do StorageGRID, o sistema poderá ter um problema com o "[configuração da federação de identidade](#)", um "[rede](#)" problema ou "[hardware](#)", um problema com "[Serviços do Admin Node](#)", ou um "[Problema com o banco de dados Cassandra](#)" em nós de armazenamento ligados.

Antes de começar

- Você tem o `Passwords.txt` arquivo.
- Você "[permissões de acesso específicas](#)" tem .

Sobre esta tarefa

Use estas diretrizes de solução de problemas se você vir qualquer uma das seguintes mensagens de erro ao tentar entrar em um nó de administrador:

- 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 iniciar sessão 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 administrador, tente fazer login no Gerenciador de Grade de outro nó de administrador.
 - Se você conseguir entrar, você pode usar as opções **Dashboard**, **Nodes**, **Alerts** e **SUPPORT** para ajudar a determinar a causa do erro.
 - Se você tiver apenas um nó Admin ou ainda não conseguir entrar, vá para a próxima etapa.
3. Determine se o hardware do nó está offline.
4. Se o logon único (SSO) estiver ativado para o sistema StorageGRID, consulte as etapas para "["configurando logon único"](#)".

Talvez seja necessário desativar e reativar temporariamente o SSO para um único nó de administração para resolver quaisquer problemas.



Se o SSO estiver ativado, você não poderá fazer logon usando uma porta restrita. Tem de utilizar 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 fazer login no Gerenciador de Grade como um usuário local, como root.

- Se o utilizador local puder iniciar sessão:
 - i. Reveja todos os alarmes apresentados.
 - ii. Selecione **CONFIGURATION > Access Control > Identity Federation**.
 - iii. Clique em **Test Connection** para validar as 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 tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.

6. Use o Secure Shell (ssh) para fazer login no Admin Node:

- a. Introduza o seguinte comando: ssh admin@Admin_Node_IP
- b. Introduza a palavra-passe listada no Passwords.txt ficheiro.
- c. Digite o seguinte comando para mudar para root: su -
- d. Introduza a palavra-passe listada no Passwords.txt ficheiro.

Quando você estiver conectado como root, o prompt mudará de \$ para #.

7. Veja 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 Lumberjack para coletar logs: # /usr/local/sbin/lumberjack.rb

Se a autenticação com falha aconteceu no passado, você pode usar as opções de script --start e --end 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. Rever 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 Admin, emita um dos seguintes comandos para determinar os endereços IP dos três nós de armazenamento que executam o serviço ADC em seu site. Em geral, esses são os primeiros três nós de storage instalados no local.

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

```
# vi /var/local/gpt-data/specs/grid.xml
```

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

12. A partir do nó Admin, efetue login em cada um dos nós de armazenamento ADC, usando os endereços IP identificados.

- a. Introduza o seguinte comando: ssh admin@grid_node_IP
- b. Introduza a palavra-passe listada no Passwords.txt ficheiro.
- c. Digite o seguinte comando para mudar para root: su -
- d. Introduza a palavra-passe listada no Passwords.txt ficheiro.

Quando você estiver conectado como root, o prompt mudará de \$ para #.

13. Veja 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 as etapas [Use Lumberjack para coletar logs](#) e [Rever registos](#) para revisar os logs nos nós de storage.

15. Se você não conseguir resolver o problema, entre em Contato com o suporte técnico.

Forneça os Registros que você coletou para o suporte técnico. Consulte também "[Referência de ficheiros de registo](#)".

Problemas na interface do usuário

A interface de usuário do Gerenciador de Grade ou do Gerenciador de Locatário pode não responder como esperado após o upgrade do software StorageGRID.

Passos

1. Certifique-se de que está a utilizar um "[navegador da web suportado](#)".



O suporte do navegador pode mudar a cada versão do StorageGRID. Confirme que você está usando um navegador compatível com a versão do StorageGRID.

2. Limpe o cache do navegador da Web.

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

Nó Admin indisponível

Se o sistema StorageGRID incluir vários nós de administração, você poderá usar outro nó de administração para verificar o status de um nó de administração indisponível.

Antes de começar

Você "[permissões de acesso específicas](#)" tem .

Passos

1. Em um nó Admin disponível, faça login no Gerenciador de Grade usando um "[navegador da web suportado](#)".
2. Selecione **SUPPORT > Tools > Grid topology**.
3. Selecione **Site > nó Admin indisponível > SSM > Serviços > Visão geral > Principal**.
4. Procure serviços que tenham um status de não execução e que também possam ser exibidos em azul.



Overview: SSM (MM-10-224-4-81-ADM1) - Services

Updated: 2017-01-27 11:52:51 EST

Operating System:

Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Audit Management System (AMS)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.043 %	35.7 MB
CIFS Filesharing (nmbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	5.5 MB
CIFS Filesharing (smbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	14.5 MB
CIFS Filesharing (winbindd)	2:4.2.14+dfsg-0+deb8u2	Not Running	0	0 %	0 B
Configuration Management Node (CMN)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.055 %	41.3 MB
Database Engine	5.5.53-0+deb8u1	Running	47	0.354 %	1.33 GB
Grid Deployment Utility Server	10.4.0-20170112.2125.c4253bb	Running	3	0 %	32.8 MB
Management Application Program Interface (mgmt-api)	10.4.0-20170113.2136.07c4997	Not Running	0	0 %	0 B
NFS Filesharing	10.4.0-20161224.0333.803cd91	Not Running	0	0 %	0 B
NMS Data Cleanup	10.4.0-20161224.0333.803cd91	Running	22	0.008 %	52.4 MB
NMS Data Downampler 1	10.4.0-20161224.0333.803cd91	Running	22	0.049 %	195 MB
NMS Data Downampler 2	10.4.0-20161224.0333.803cd91	Running	22	0.009 %	157 MB
NMS Processing Engine	10.4.0-20161224.0333.803cd91	Running	40	0.132 %	200 MB

- Determine se os alarmes foram acionados.
- Tome as medidas apropriadas para resolver o problema.

Solucionar problemas de rede, hardware e plataforma

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

"422: Entidade não processável" erros

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

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

Mensagem de erro	Causa raiz e ação corretiva
<p>422: Unprocessable Entity</p> <p>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</p>	<p>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 ative Directory (AD).</p> <p>O uso da opção não usar TLS não é suportado para uso com servidores AD que imponham a assinatura LDAP. Você deve selecionar a opção usar STARTTLS ou a opção usar LDAPS para TLS.</p>
<p>422: Unprocessable Entity</p> <p>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)</p>	<p>Essa mensagem será exibida 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 pools de federação ou armazenamento em nuvem.</p> <p>Verifique as cifras que são oferecidas pelo sistema externo. O sistema deve usar um dos "Cifras suportadas por StorageGRID" para conexões TLS de saída, como mostrado nas instruções de administração do StorageGRID.</p>

Alerta de incompatibilidade da MTU da rede de Grade

O alerta **Grid Network MTU mismatch** é acionado quando a configuração MTU (unidade máxima de transmissão) para a interface Grid Network (eth0) difere significativamente entre nós na grade.

Sobre esta tarefa

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

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
 - Use a consulta fornecida no Gerenciador de Grade.
 - Navegue para *primary Admin Node IP address/metrics/graph* e insira a seguinte consulta:
node_network_mtu_bytes{device="eth0"}
2. **"Modifique as configurações MTU"** Conforme necessário para garantir que eles sejam iguais para a interface de rede de Grade (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`

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

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

Argumentos posicionais	Descrição
<code>mtu</code>	A MTU a definir. Deve estar na faixa de 1280 a 9216.
<code>network</code>	As redes às quais aplicar a MTU. Inclua um ou mais dos seguintes tipos de rede: <ul style="list-style-type: none">◦ <code>grelha</code>◦ <code>administrador</code>◦ <code>cliente</code>

+

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

Alarme de erro de receção de rede (NRER)

Os alarmes de erro de receção de rede (NRER) podem ser causados por problemas de conectividade entre o StorageGRID e o hardware da rede. Em alguns casos, erros NRER podem ser claros sem intervenção manual. Se os erros não forem claros, execute as ações recomendadas.

Sobre esta tarefa

Os alarmes NRER podem ser causados pelos seguintes problemas com o hardware de rede que se conecta ao

StorageGRID:

- A correção de erro de avanço (FEC) é necessária e não está em uso
- Incompatibilidade da MTU da porta do switch e da NIC
- Altas taxas de erro de link
- Buffer de anel NIC excedido

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas do alarme NRER, dada a configuração da rede.
2. Execute as seguintes etapas, dependendo da causa do erro:

Incompatibilidade de FEC



Estes passos são aplicáveis apenas para erros NRER causados por incompatibilidade de FEC em dispositivos StorageGRID.

- a. Verifique o status do FEC da porta no switch conectado ao seu dispositivo StorageGRID.
- b. Verifique a integridade física dos cabos do aparelho ao interruptor.
- c. Se pretender alterar as definições do FEC para tentar resolver o alarme NRER, certifique-se primeiro de que o aparelho está configurado para o modo **Auto** na página Configuração de ligação do Instalador de dispositivos StorageGRID (consulte as instruções do seu aparelho):
 - ["SG6160"](#)
 - ["SGF6112"](#)
 - ["SG6000"](#)
 - ["SG5800"](#)
 - ["SG5700"](#)
 - ["SG110 e SG1100"](#)
 - ["SG100 e SG1000"](#)
- d. Altere as configurações do FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações FEC para corresponder, se possível.

Não é possível configurar as configurações do FEC nos dispositivos StorageGRID. Em vez disso, os aparelhos tentam descobrir e espelhar as configurações 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 poderão não conseguir negociar uma configuração FEC comum. Sem uma configuração FEC comum, a rede voltará para o modo "no-FEC". Quando o FEC não está ativado, as conexões são mais suscetíveis a erros causados por ruído elétrico.



A StorageGRID Appliances apoia a FEC (FC) e a FEC (RS), bem como a FEC.

Incompatibilidade da MTU da porta do switch e da NIC

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

O tamanho da MTU configurado no nó pode ser menor do que a configuração na porta do switch à qual o nó está conectado. Se um nó StorageGRID receber um quadro Ethernet maior que o MTU, o que é possível com esta configuração, o alarme NRER pode ser comunicado. Se você acredita que isso está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede da StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo dos seus objetivos ou requisitos de MTU de ponta a ponta.



Para obter o melhor desempenho de rede, todos os nós devem ser configurados com valores 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 para a rede de Grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Consulte [Solução para o alerta de incompatibilidade de MTU da rede de Grade](#) para obter mais informações.



Consulte também ["Altere a definição MTU"](#).

Altas taxas de erro de link

- a. Ative o FEC, se ainda não estiver ativado.
- b. Verifique se o cabeamento de rede é de boa qualidade e não está danificado ou conectado incorretamente.
- c. Se os cabos parecerem não ser o problema, contacte o suporte técnico.



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

Buffer de anel NIC excedido

Se o erro for uma sobrecarga do buffer do anel da NIC, entre em Contato com o suporte técnico.

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

3. Depois de resolver o problema subjacente, redefina o contador de erros.

- a. Selecione **SUPPORT > Tools > Grid topology**.
- b. Selecione **site > grid node > SSM > Resources > Configuration > Main**.
- c. Selecione **Redefinir contagem de erros de recebimento** e clique em **aplicar alterações**.

Informações relacionadas

["Referência de alarmes \(sistema legado\)"](#)

Erros de sincronização de tempo

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

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



"Especificando a fonte NTP externa" Quando for 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 StorageGRID hospedados em hosts Linux.

Clonagem de endereços MAC

Em alguns casos, os problemas de rede podem ser resolvidos usando a clonagem de endereços MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereços MAC para cada uma de suas redes como "verdadeiro" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contentor 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 contentor StorageGRID pode fazer com que o sistema operacional do host se torne inacessível se o modo promíscuo não tiver sido ativado no hypervisor.

Para obter mais informações sobre como ativar a clonagem MAC, consulte as instruções para ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#).

Modo promíscuo

Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. 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 como usar o 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 um estado órfão geralmente indica que o serviço StorageGRID ou o daemon de nó StorageGRID que controla o contentor do nó morreram inesperadamente.

Sobre esta tarefa

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

- Verifique os logs para ver se há erros e mensagens.
- Tente iniciar o nó novamente.
- Se necessário, use comandos do mecanismo do contentor para parar o contentor do nó existente.
- Reinicie o nó.

Passos

1. Verifique os logs do serviço daemon e do nó órfão para ver se há erros óbvios ou mensagens sobre sair inesperadamente.
2. Faça login no host como root ou usando 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 estiver órfão, a resposta será

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

4. A partir do Linux, pare o mecanismo de container e quaisquer processos de controle do StorageGRID-node. Por exemplo:`sudo docker stop --time seconds container-name`

Para seconds, introduza o número de segundos que pretende aguardar que o recipiente 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: Solucione problemas de suporte ao IPv6

Talvez seja necessário habilitar o suporte IPv6 no kernel se você tiver instalado nós do StorageGRID em hosts Linux e notar que os endereços IPv6 não foram atribuídos aos contentores do nó como esperado.

Sobre esta tarefa

Você pode ver o endereço IPv6 que foi atribuído a um nó de grade nos seguintes locais no Gerenciador de Grade:

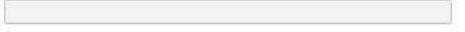
- Selecione **NÓS** e selecione o nó. Em seguida, selecione **Mostrar mais** ao lado de **endereços IP** na guia Visão geral.

DC1-S2 (Storage Node) 



Overview  Hardware Network Storage Objects ILM Tasks

Node information 

Name:	DC1-S2						
Type:	Storage Node						
ID:	352bd978-ff3e-45c5-aac1-24c7278206fa						
Connection state:	 Connected						
Storage used:	Object data  0%  Object metadata  0% 						
Software version:	11.6.0 (build 20210924.1557.00a5eb9)						
IP addresses:	172.16.1.227 - eth0 (Grid Network) 10.224.1.227 - eth1 (Admin Network)						
Hide additional IP addresses 							
<table border="1"> <thead> <tr> <th>Interface</th> <th>IP address</th> </tr> </thead> <tbody> <tr> <td>eth0 (Grid Network)</td> <td>172.16.1.227</td> </tr> <tr> <td>eth0 (Grid Network)</td> <td>fd20:328:328:0:250:56ff:fe87:b532</td> </tr> </tbody> </table>		Interface	IP address	eth0 (Grid Network)	172.16.1.227	eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532
Interface	IP address						
eth0 (Grid Network)	172.16.1.227						
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532						

- Selecione **SUPPORT > Tools > Grid topology**. Em seguida, selecione **node > SSM > Resources**. Se um endereço IPv6 tiver sido atribuído, ele será listado abaixo do endereço IPv4 na seção **endereços de rede**.

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

- Faça login no host como root ou usando uma conta com permissão sudo.
- 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 sistema operacional para alterar `sysctl` as configurações. Em seguida, altere o valor para 0 antes de continuar.

- Insira o contentor 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. Saia do recipiente: `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 contentor 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	<p>O FQDN inserido para o servidor syslog não pôde ser resolvido para um endereço IP.</p> <ol style="list-style-type: none">1. Verifique o nome do host que você inseriu. Se você inseriu um endereço IP, certifique-se de que é um endereço IP válido na notação W.X.Y.Z ("decimal pontilhado").2. Verifique se os servidores DNS estão configurados corretamente.3. Confirme se cada nó pode acessar os endereços IP do servidor DNS.
Ligação recusada	<p>Uma conexão TCP ou TLS ao servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS para o host, ou um firewall pode estar bloqueando o acesso.</p> <ol style="list-style-type: none">1. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo 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 a conexões TCP/TLS dos nós para o IP e a porta do servidor syslog.
Rede inacessível	<p>O servidor syslog não está em uma sub-rede conectada diretamente. Um roteador retornou uma mensagem de falha ICMP para indicar que não foi possível encaminhar as mensagens de teste dos nós listados para o servidor syslog.</p> <ol style="list-style-type: none">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 de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog através da interface de rede e gateway esperados (Grid, Admin ou Client).

Mensagem de erro	Descrição e ações recomendadas
Host inalcançável	<p>O servidor syslog está em uma sub-rede conectada diretamente (sub-rede usada pelos nós listados para seus endereços IP de Grade, Admin ou Cliente). Os nós tentaram enviar mensagens de teste, mas não receberam respostas a solicitações ARP para o endereço MAC do servidor syslog.</p> <ol style="list-style-type: none"> 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 ligação esgotado	<p>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 deixando cair o tráfego sem enviar qualquer resposta (uma configuração comum).</p> <ol style="list-style-type: none"> 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 de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog usando a interface de rede e gateway (Grid, Admin ou Client) sobre o qual você espera que o servidor syslog seja alcançado. 3. Confirme se um firewall não está bloqueando o acesso a conexões TCP/TLS dos nós listados para o IP e a porta do servidor syslog.
Conexão fechada pelo parceiro	<p>Uma conexão TCP ao servidor syslog foi estabelecida com êxito, mas foi fechada mais tarde. As razões para isso podem incluir:</p> <ul style="list-style-type: none"> • O servidor syslog pode ter sido reiniciado ou reiniciado. • O nó e o servidor syslog podem ter configurações diferentes de TCP/TLS. • Um firewall intermediário pode estar fechando conexões TCP ociosas. • Um servidor que não seja syslog escutando na porta do servidor syslog pode ter fechado a conexão. <p>Para resolver este problema:</p> <ol style="list-style-type: none"> 1. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo 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	<p>O certificado de servidor recebido do servidor syslog não era compatível com o pacote de certificados CA e o certificado de cliente fornecido.</p> <ol style="list-style-type: none"> 1. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor syslog. 2. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Reencaminhamento suspenso	<p>Os Registros do syslog não estão mais sendo encaminhados para o servidor syslog e o StorageGRID não consegue detetar o motivo.</p> <p>Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz.</p>
Sessão TLS terminada	<p>O servidor syslog encerrou a sessão TLS e o StorageGRID não consegue detetar o motivo.</p> <ol style="list-style-type: none"> 1. Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz. 2. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo 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 syslog. 5. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Falha na consulta de resultados	<p>O nó Admin usado para configuração e teste do servidor syslog não consegue solicitar resultados de teste dos nós listados. Um ou mais nós podem estar inativos.</p> <ol style="list-style-type: none"> 1. Siga as etapas padrão de solução de problemas para garantir que os nós estejam online e que todos os serviços esperados estejam em execução. 2. Reinicie o serviço miscd nos nós listados.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.