Monitorar e solucionar problemas

StorageGRID software

NetApp
December 03, 2025

Índice

Monitorar e solucionar problemas de um sistema StorageGRID

Monitorar o sistema StorageGRID

Monitorar um sistema StorageGRID

Monitore seu sistema StorageGRID regularmente para garantir que ele esteja funcionando conforme o esperado.

Antes de começar

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

> Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.

Sobre esta tarefa

Estas instruções descrevem como:

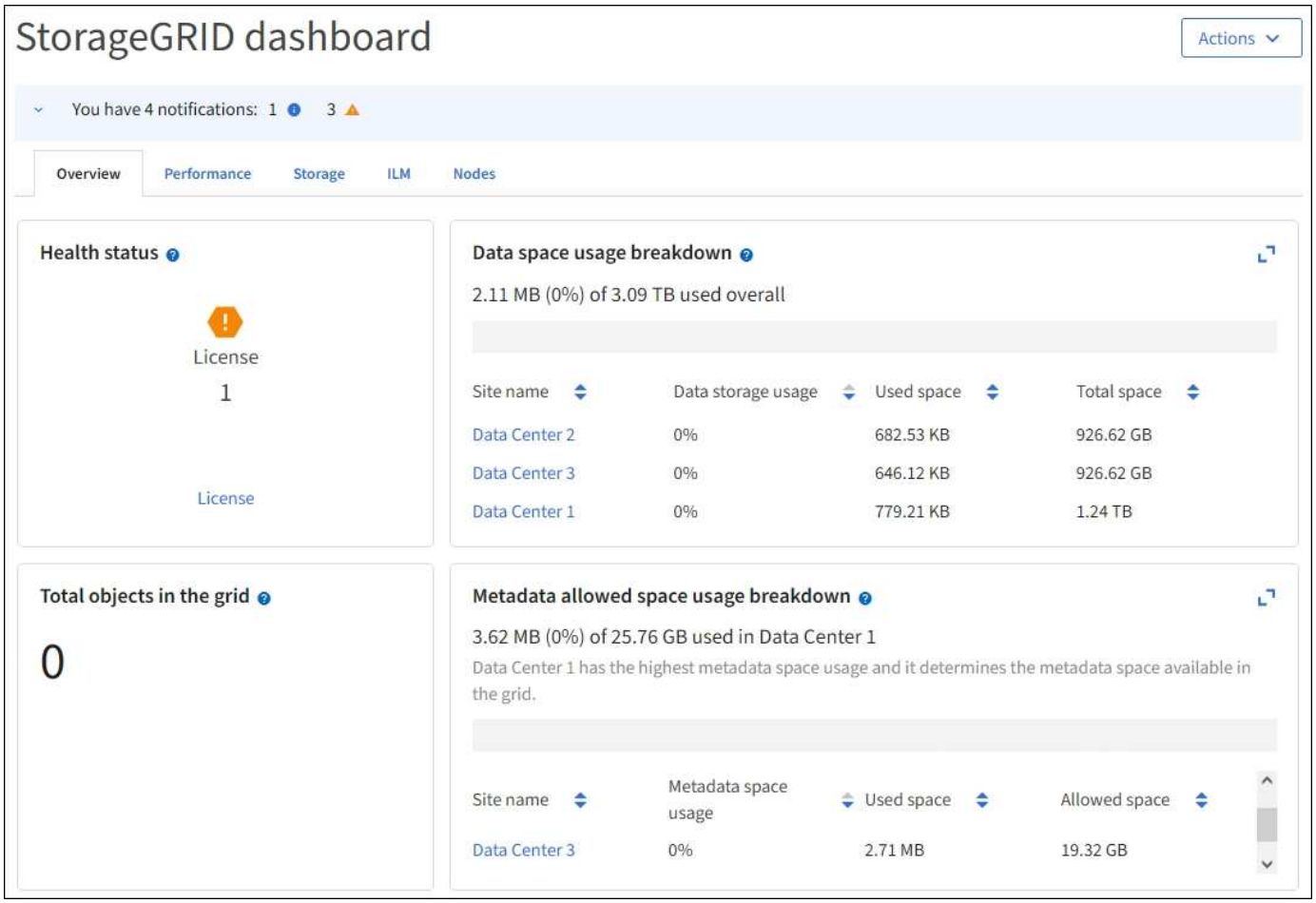
- "Visualizar e gerenciar o painel"
- "Ver a página de nós"
- "Monitore estes aspectos do sistema regularmente:"
  - "Saúde do sistema"
  - "Capacidade de armazenamento"
  - "Gestão do ciclo de vida da informação"
  - "Recursos de rede e sistema"
  - "Atividade do inquilino"
  - "Operações de balanceamento de carga"
  - "Conexões de federação de rede"
- "Gerenciar alertas"
- "Ver arquivos de log"
- "Configurar mensagens de auditoria e destinos de log"
- "Use um servidor syslog externo"para coletar informações de auditoria
- "Use SNMP para monitoramento"
- "Obter dados adicionais do StorageGRID", incluindo métricas e diagnósticos

Visualizar e gerenciar o painel

Você pode usar o painel para monitorar as atividades do sistema rapidamente. Você pode criar painéis personalizados para monitorar sua implementação do StorageGRID.

Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.

Seu painel pode ser diferente dependendo da configuração do sistema.



Ver o painel

O painel consiste em guias que contêm informações específicas sobre o sistema StorageGRID . Cada aba contém categorias de informações exibidas nos cartões.

Você pode usar o painel fornecido pelo sistema como está. Além disso, você pode criar painéis personalizados que contenham apenas as guias e os cartões relevantes para monitorar sua implementação do StorageGRID.

As guias do painel fornecidas pelo sistema contêm cartões com os seguintes tipos de informações:

Guia no painel fornecido pelo sistema	Contém
Visão geral	Informações gerais sobre a grade, como alertas ativos, uso de espaço e total de objetos na grade.

Guia no painel fornecido pelo sistema	Contém
Desempenho	Uso de espaço, armazenamento usado ao longo do tempo, operações S3, duração da solicitação, taxa de erro.
Armazenar	Uso de cota de locatário e uso de espaço lógico. Previsões de uso do espaço para dados e metadados do usuário.
ILM	Fila de gerenciamento do ciclo de vida da informação e taxa de avaliação.
Nós	Uso de CPU, dados e memória por nó. Operações S3 por nó. Distribuição de nó para site.

Alguns cartões podem ser maximizados para facilitar a visualização. Selecione o ícone maximizar no canto superior direito do cartão. Para fechar um cartão maximizado, selecione o ícone de minimizar ou selecione **Fechar**.

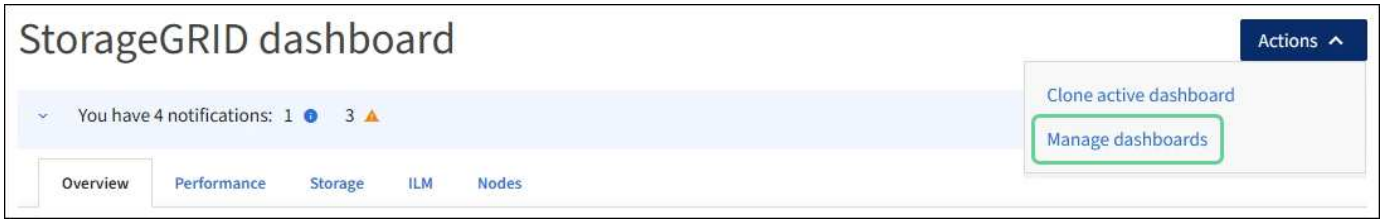
Gerenciar painéis

Se você tiver acesso Root (veja"Permissões do grupo de administração"), você pode executar as seguintes tarefas de gerenciamento para painéis:

- Crie um painel personalizado do zero. Você pode usar painéis personalizados para controlar quais informações do StorageGRID são exibidas e como essas informações são organizadas.
- Clone um painel para criar painéis personalizados.
- Defina um painel ativo para um usuário. O painel ativo pode ser o painel fornecido pelo sistema ou um painel personalizado.
- Defina um painel padrão, que é o que todos os usuários veem, a menos que ativem seu próprio painel.
- Editar um nome de painel.
- Edite um painel para adicionar ou remover guias e cartões. Você pode ter no mínimo 1 e no máximo 20 abas.
- Remover um painel.

Se você tiver qualquer outra permissão além do acesso Root, você só poderá definir um painel ativo.

Para gerenciar painéis, selecione **Ações** > **Gerenciar painéis**.



Configurar painéis

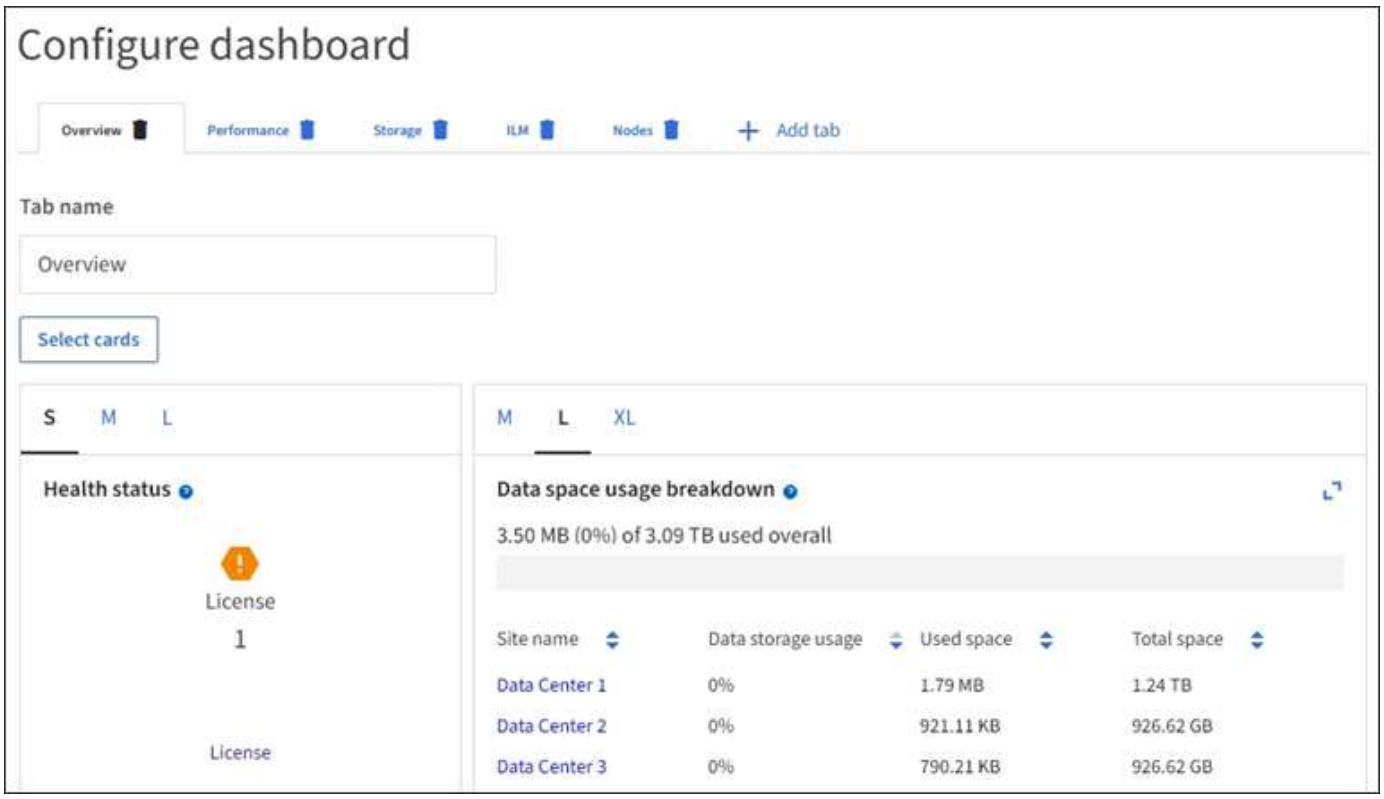
Para criar um novo painel clonando o painel ativo, selecione **Ações** > **Clonar painel ativo**.

Para editar ou clonar um painel existente, selecione **Ações** > **Gerenciar painéis**.

O painel fornecido pelo sistema não pode ser editado ou removido.

Ao configurar um painel, você pode:

- Adicionar ou remover guias
- Renomeie as guias e dê nomes exclusivos às novas guias
- Adicionar, remover ou reorganizar (arrastar) cartões para cada guia
- Selecione o tamanho dos cartões individuais selecionando **P**, **M**, **G** ou **GG** na parte superior do cartão



Ver a página de nós

Ver a página de nós

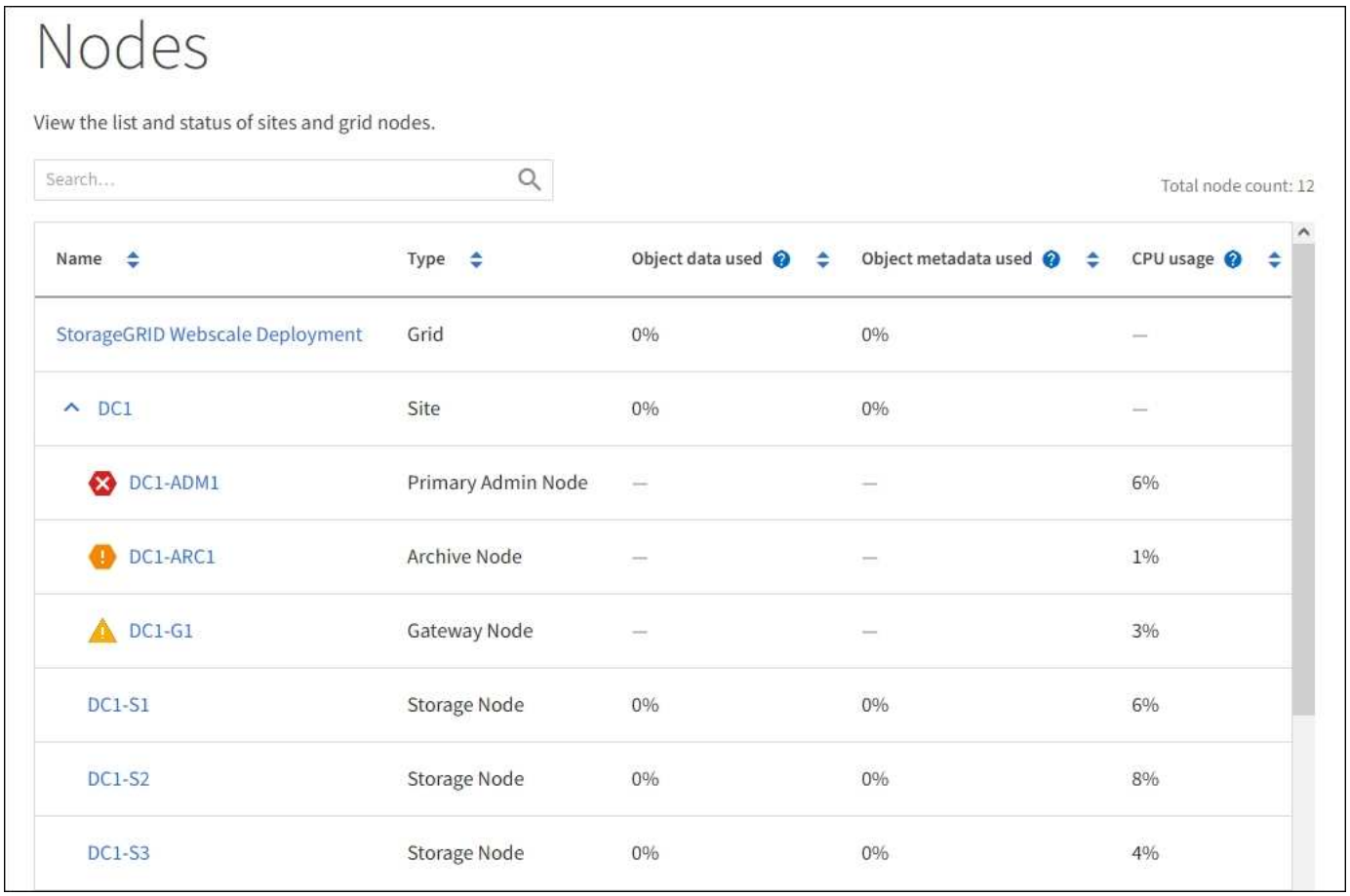
Quando precisar de informações mais detalhadas sobre seu sistema StorageGRID do que o painel fornece, você pode usar a página Nós para visualizar métricas para toda a grade, cada site na grade e cada nó em um site.

A tabela Nós lista informações resumidas para toda a grade, cada site e cada nó. Se um nó estiver desconectado ou tiver um alerta ativo, um ícone aparecerá ao lado do nome do nó. Se o nó estiver conectado e não tiver alertas ativos, nenhum ícone será exibido.

Quando um nó não está conectado à rede, como durante uma atualização ou em um estado desconectado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da rede. Depois que um nó se reconectar à rede, aguarde alguns minutos para que os valores se estabilizem.

Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.

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



Ícones de estado de conexão

Se um nó for desconectado da grade, um dos seguintes ícones aparecerá ao lado do nome do nó.

Ícone	Descrição	Ação necessária
	**Não conectado - Desconhecido** Por um motivo desconhecido, um nó é desconectado ou os serviços no nó ficam inesperadamente inativos. Por exemplo, um serviço no nó pode ser interrompido, ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta **Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. "Selecione cada alerta" e siga as ações recomendadas. Por exemplo, talvez seja necessário reiniciar um serviço que foi interrompido ou reiniciar o host do nó. **Observação**: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	**Não conectado - Inativo administrativamente** Por um motivo esperado, o nó não está conectado à rede. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Determine se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos,"Selecione cada alerta" e siga as ações recomendadas.

Se um nó estiver desconectado da rede, poderá haver um alerta subjacente, mas somente o ícone "Não conectado" aparecerá. Para ver os alertas ativos de um nó, selecione o nó.

Ícones de alerta

Se houver um alerta ativo para um nó, um dos seguintes ícones aparecerá ao lado do nome do nó:

 **Crítico**: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido.

 **Principal**: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID .

 **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.

Exibir detalhes de um sistema, site ou nó

Para filtrar as informações mostradas na tabela Nós, insira uma sequência de pesquisa no campo **Pesquisar**. Você pode pesquisar por nome do sistema, nome de exibição ou tipo (por exemplo, digite **gat** para localizar rapidamente todos os nós de gateway).

Para visualizar as informações da grade, site ou nó:

- Selecione o nome da grade para ver um resumo agregado das estatísticas de todo o seu sistema StorageGRID .
- Selecione um site de data center específico para ver um resumo agregado das estatísticas de todos os nós naquele site.
- Selecione um nó específico para visualizar informações detalhadas sobre ele.

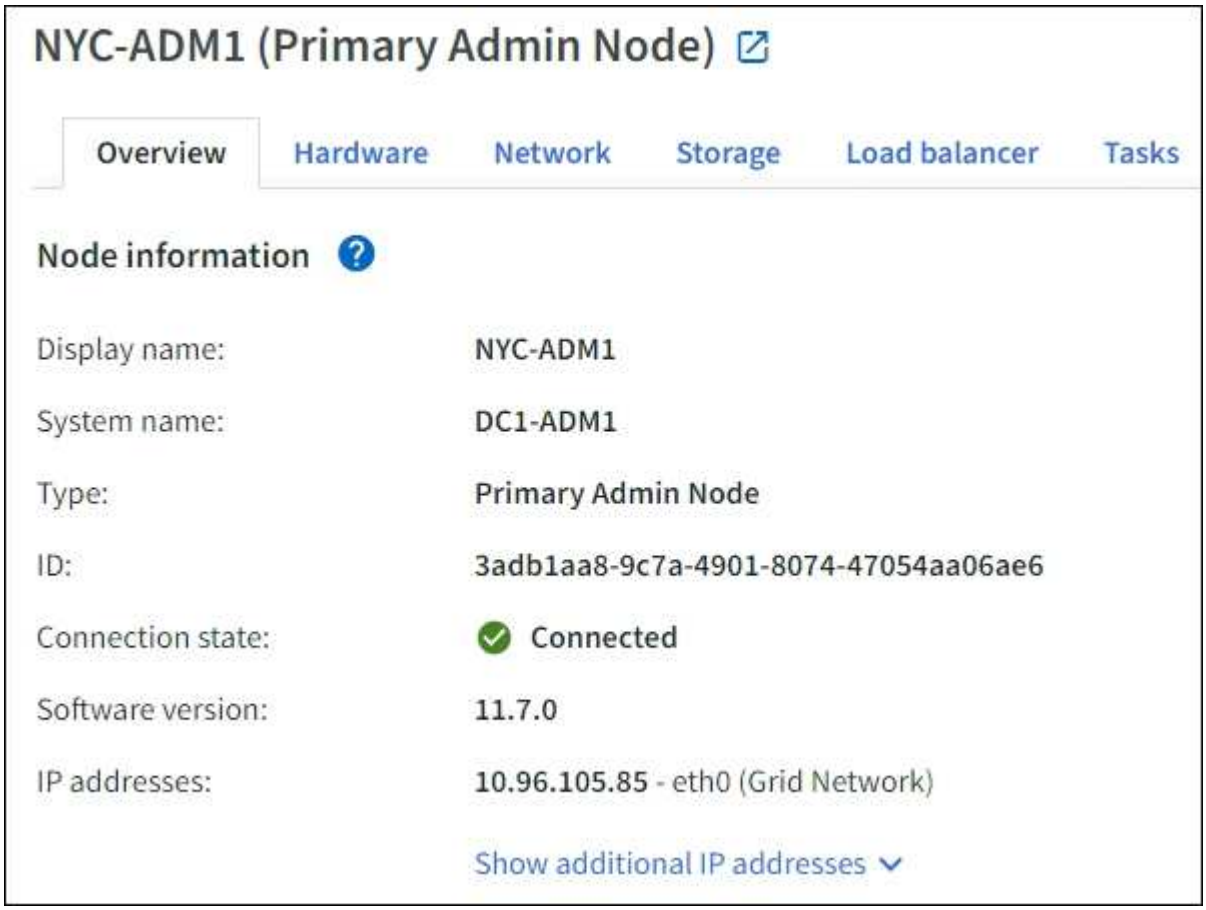
Exibir a guia Visão geral

A guia Visão geral fornece informações básicas sobre cada nó. Ele também mostra todos os alertas que estão afetando o nó no momento.

A guia Visão geral é exibida para todos os nós.

Informações do nó

A seção Informações do nó da guia Visão geral lista informações básicas sobre o nó.



As informações gerais de um nó incluem o seguinte:

- **Nome de exibição** (mostrado somente se o nó tiver sido renomeado): O nome de exibição atual do nó. Use o"Renomear grade, sites e nós" procedimento para atualizar este valor.
- **Nome do sistema**: O nome que você inseriu para o nó durante a instalação. Os nomes do sistema são usados para operações internas do StorageGRID e não podem ser alterados.
- **Tipo**: O tipo de nó — Nó de administração, Nó de administração primário, Nó de armazenamento ou Nó de gateway.
- **ID**: O identificador exclusivo do nó, também conhecido como UUID.
- **Estado da conexão**: Um dos três estados. O ícone para o estado mais grave é mostrado.
  - **Desconhecido*** **: Por um motivo desconhecido, o nó não está conectado à rede ou um ou mais serviços estão inesperadamente inativos. Por exemplo, a conexão de rede entre os nós foi perdida, a energia caiu ou um serviço caiu. O alerta *Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.

    Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.

  - *Administrativamente inativo* : O nó não está conectado à rede por um motivo esperado. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.
  - *Conectado* : O nó está conectado à rede.
- **Armazenamento usado**: somente para nós de armazenamento.
  - **Dados do objeto**: A porcentagem do espaço total utilizável para dados do objeto que foi usada no nó de armazenamento.
  - **Metadados do objeto**: A porcentagem do espaço total permitido para metadados do objeto que foi usada no nó de armazenamento.
- **Versão do software**: A versão do StorageGRID que está instalada no nó.
- **Grupos HA**: somente para nós de administração e nós de gateway. Mostrado se uma interface de rede no nó está incluída em um grupo de alta disponibilidade e se essa interface é a interface primária.
- **Endereços IP**: Endereços IP do nó. Clique em **Mostrar endereços IP adicionais** para visualizar os endereços IPv4 e IPv6 do nó e os mapeamentos de interface.

Alertas

A seção Alertas da guia Visão geral lista qualquer"alertas que atualmente afetam este nó e que não foram silenciados" . Selecione o nome do alerta para ver detalhes adicionais e ações recomendadas.

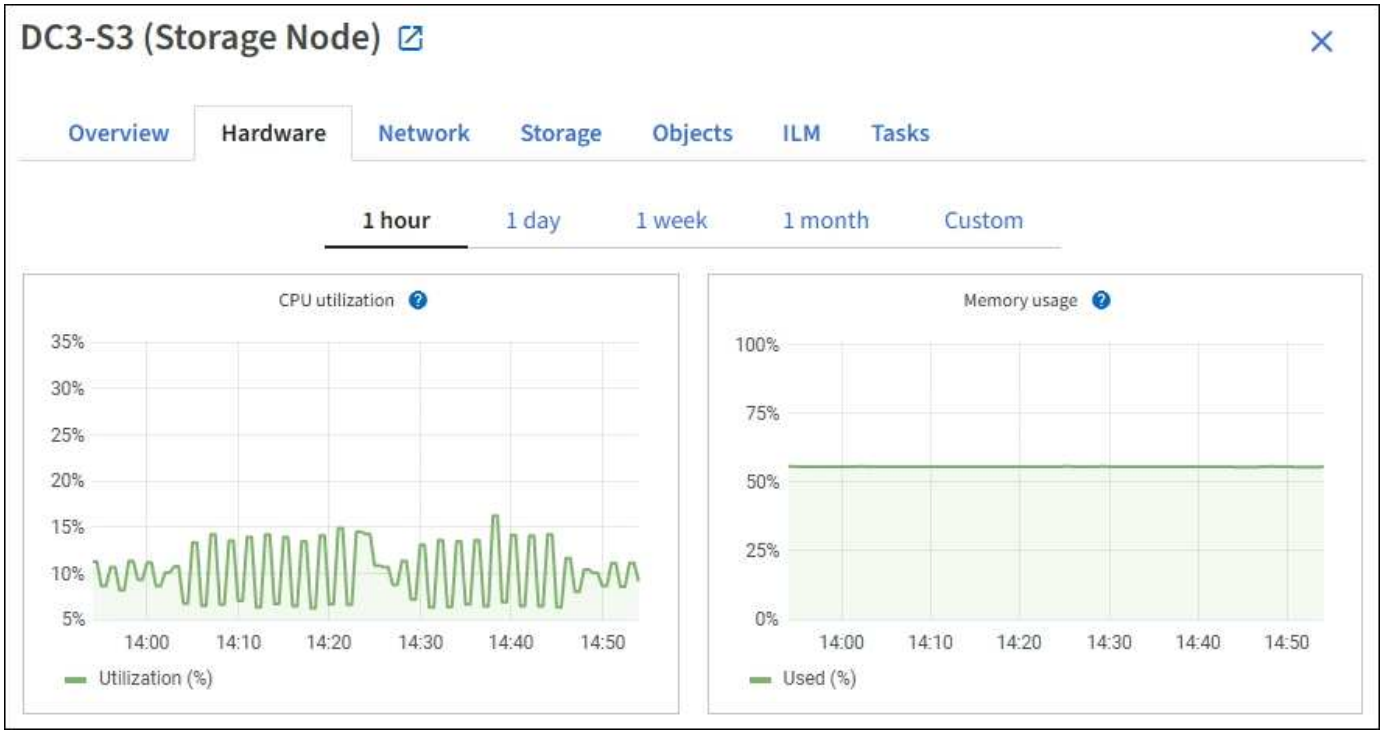
Alertas também estão incluídos para"estados de conexão do nó" .

Ver a aba Hardware

A guia Hardware exibe a utilização da CPU e da memória para cada nó, além de informações adicionais de hardware sobre os dispositivos.

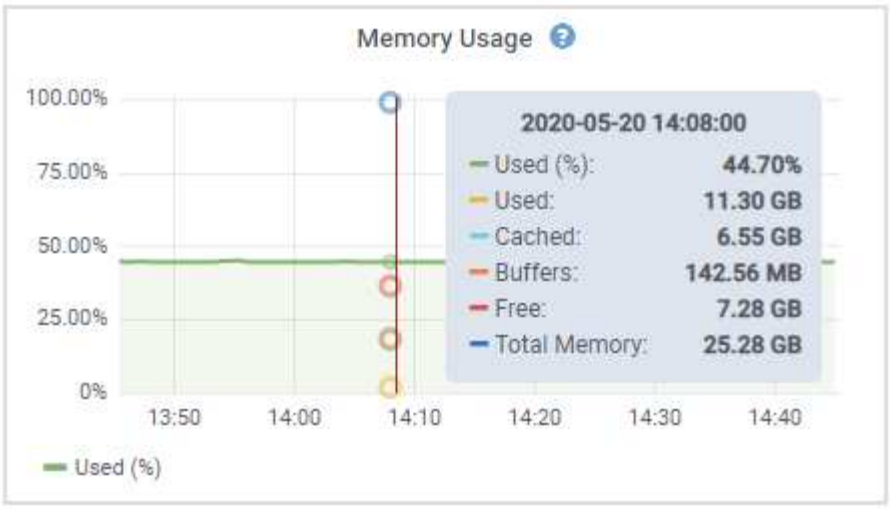
> O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A guia Hardware é exibida para todos os nós.



Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.

Para ver detalhes sobre a utilização da CPU e da memória, posicione o cursor sobre cada gráfico.



Se o nó for um nó de dispositivo, esta guia também incluirá uma seção com mais informações sobre o hardware do dispositivo.

Exibir informações sobre nós de armazenamento do dispositivo

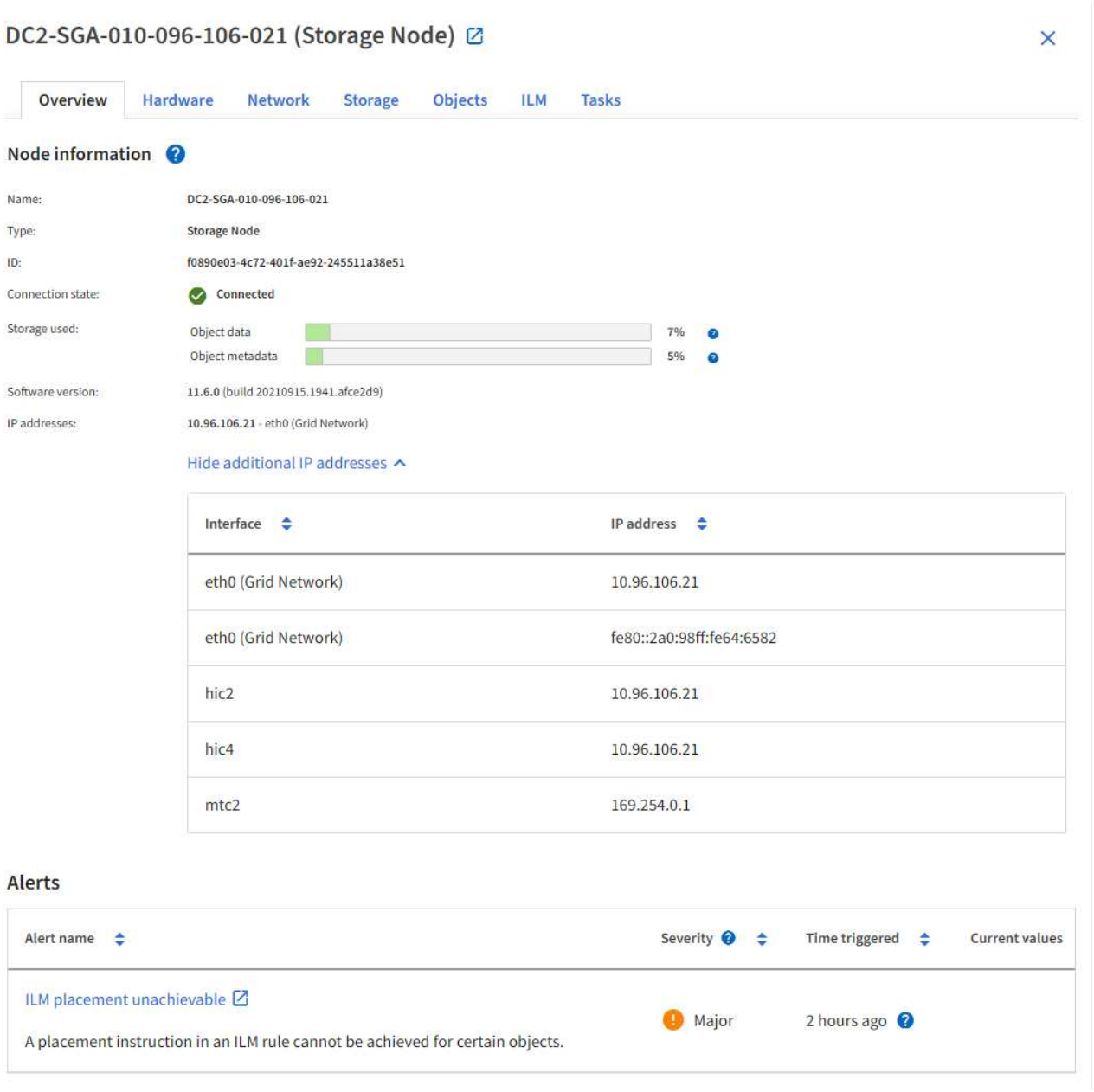
A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada nó de armazenamento do dispositivo. Você também pode ver memória, hardware de armazenamento, versão de firmware do controlador, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

Passos

1. Na página Nós, selecione um Nó de Armazenamento do dispositivo.
2. Selecione **Visão geral**.

   A seção Informações do nó da guia Visão geral exibe informações resumidas do nó, como nome, tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte forma:

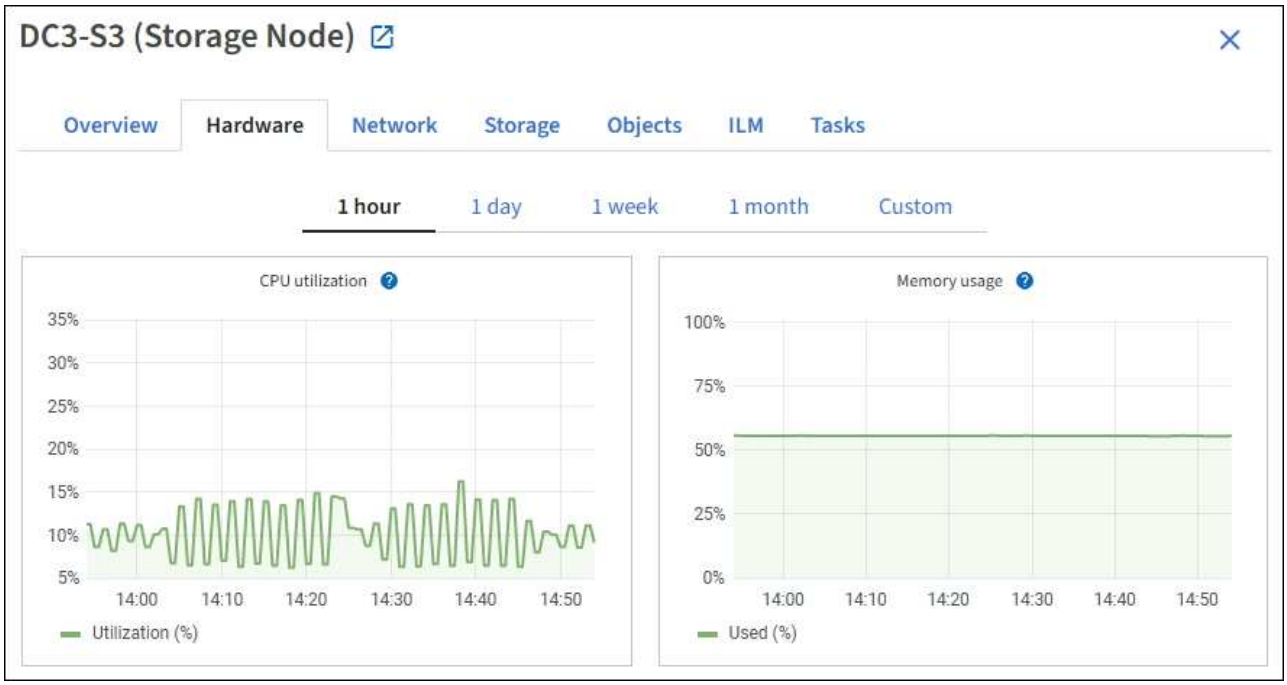
   - **eth**: Rede Grid, Rede Admin ou Rede Cliente.
   - **soluço**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Essas portas podem ser vinculadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
   - **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são vinculadas para formar a interface de rede de administração do StorageGRID (eth1). Você pode deixar outras interfaces mtc disponíveis para conectividade local temporária para um técnico no data center.



A seção Alertas da guia Visão geral exibe todos os alertas ativos para o nó.

3. Selecione **Hardware** para ver mais informações sobre o aparelho.

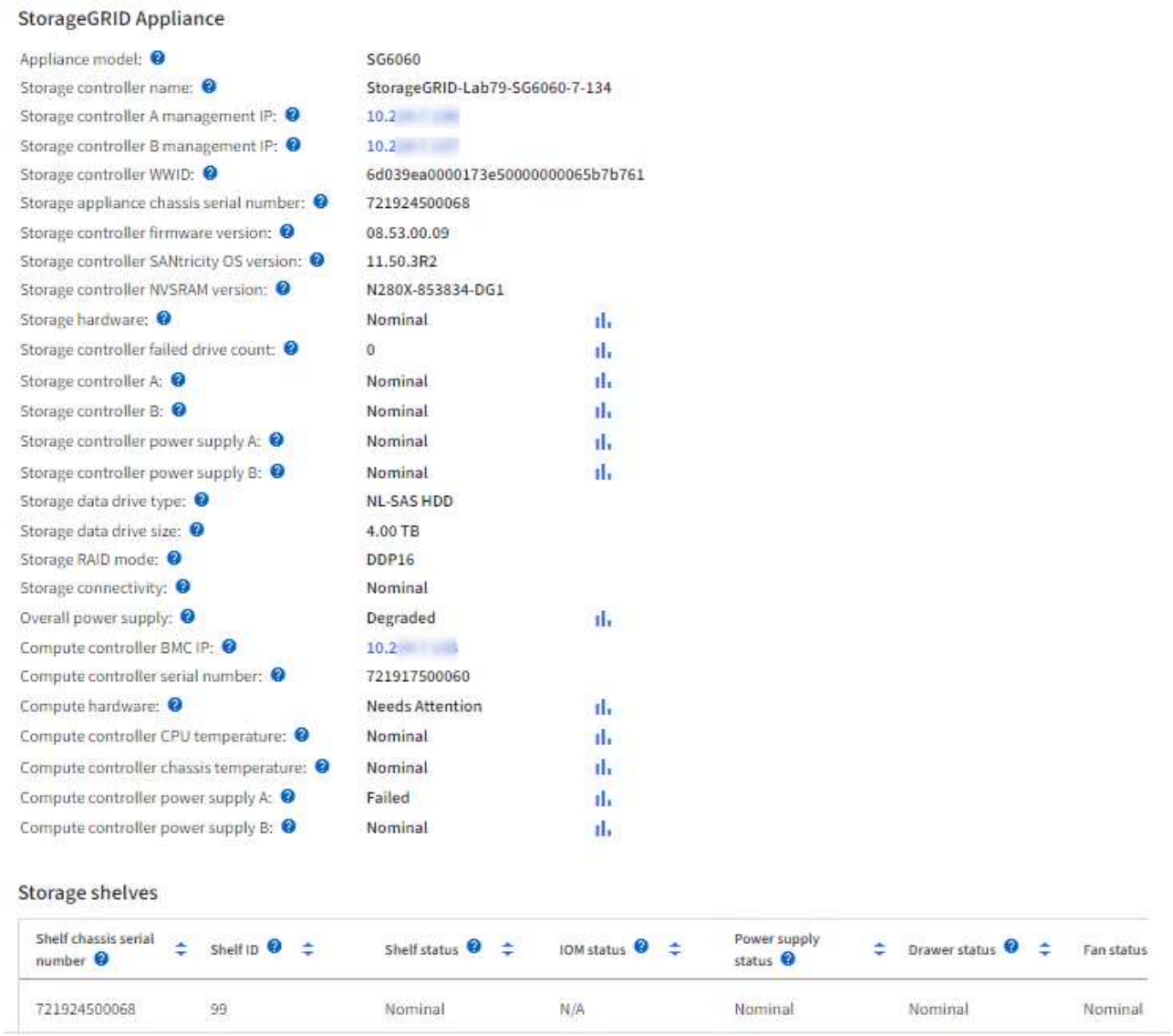
   a. Visualize os gráficos de Utilização da CPU e Memória para determinar as porcentagens de uso da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.



b. Role para baixo para ver a tabela de componentes do aparelho. Esta tabela contém informações como o nome do modelo do dispositivo; nomes dos controladores, números de série e endereços IP; e o status de cada componente.

> Alguns campos, como IP do BMC do controlador de computação e Hardware de computação, aparecem somente para dispositivos com esse recurso.

Os componentes das prateleiras de armazenamento e das prateleiras de expansão, se fizerem parte da instalação, aparecem em uma tabela separada abaixo da tabela do aparelho.



Campo na tabela Appliance	Descrição
Modelo do aparelho	O número do modelo deste dispositivo StorageGRID mostrado no SANtricity OS.
Nome do controlador de armazenamento	O nome deste dispositivo StorageGRID mostrado no SANtricity OS.
Controlador de armazenamento Um IP de gerenciamento	Endereço IP para a porta de gerenciamento 1 no controlador de armazenamento A. Use esse IP para acessar o SANtricity OS para solucionar problemas de armazenamento.
IP de gerenciamento do controlador de armazenamento B	Endereço IP para a porta de gerenciamento 1 no controlador de armazenamento B. Use esse IP para acessar o SANtricity OS para solucionar problemas de armazenamento. Alguns modelos de aparelhos não possuem um controlador de armazenamento B.

Campo na tabela Appliance	Descrição
Controlador de armazenamento WWID	O identificador mundial do controlador de armazenamento mostrado no SANtricity OS.
Número de série do chassi do dispositivo de armazenamento	O número de série do chassi do aparelho.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento para este dispositivo.
Controlador de armazenamento SANtricity versão do sistema operacional	A versão do controlador de armazenamento A do SANtricity OS.
Versão NVSRAM do controlador de armazenamento	Versão NVSRAM do controlador de armazenamento, conforme relatado pelo SANtricity System Manager. Para o SG6060 e o SG6160, se houver uma incompatibilidade de versão NVSRAM entre os dois controladores, a versão do controlador A será exibida. Se o controlador A não estiver instalado ou operacional, a versão do controlador B será exibida.
Hardware de armazenamento	O status geral do hardware do controlador de armazenamento. Se o SANtricity System Manager relatar um status de Necessita de Atenção para o hardware de armazenamento, o sistema StorageGRID também relatará esse valor. Se o status for "precisa de atenção", primeiro verifique o controlador de armazenamento usando o SANtricity OS. Em seguida, certifique-se de que não haja outros alertas aplicáveis ao controlador de computação.
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não são ideais.
Controlador de armazenamento A	O status do controlador de armazenamento A.
Controlador de armazenamento B	O status do controlador de armazenamento B. Alguns modelos de dispositivos não têm um controlador de armazenamento B.
Fonte de alimentação do controlador de armazenamento A	O status da fonte de alimentação A para o controlador de armazenamento.
Fonte de alimentação do controlador de armazenamento B	O status da fonte de alimentação B para o controlador de armazenamento.

Campo na tabela Appliance	Descrição
Tipo de unidade de armazenamento de dados	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados. No SG6160, o tamanho da unidade de cache também é exibido. **Observação**: Para nós com prateleiras de expansão, use oTamanho da unidade de dados para cada prateleira em vez de. O tamanho efetivo da unidade pode variar de acordo com a prateleira.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de armazenamento	O estado de conectividade de armazenamento.
Fonte de alimentação geral	O status de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento da placa base (BMC) no controlador de computação. Use esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é exibido para modelos de aparelhos que não contêm um BMC.
Calcular o número de série do controlador	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação. Este campo não é exibido para modelos de dispositivos que não têm hardware de computação e hardware de armazenamento separados.
Controlador de computação de temperatura da CPU	O status da temperatura da CPU do controlador de computação.
Calcular a temperatura do chassi do controlador	O status da temperatura do controlador de computação.

+

Coluna na mesa de prateleiras de armazenamento	Descrição
Número de série do chassi da prateleira	O número de série do chassi da prateleira de armazenamento.

Coluna na mesa de prateleiras de armazenamento	Descrição
ID da prateleira	O identificador numérico da prateleira de armazenamento. • 99: Prateleira do controlador de armazenamento • 0: Primeira prateleira de expansão • 1: Segunda prateleira de expansão **Observação:** Prateleiras de expansão se aplicam somente ao SG6060 e SG6160.
Status da prateleira	O status geral da prateleira de armazenamento.
Status da OIM	O status dos módulos de entrada/saída (IOMs) em quaisquer prateleiras de expansão. N/A se esta não for uma prateleira de expansão.
Status da fonte de alimentação	Status geral das fontes de alimentação da prateleira de armazenamento.
Status da gaveta	O status das gavetas na prateleira de armazenamento. N/A se a prateleira não contiver gavetas.
Status do fã	O status geral dos ventiladores de resfriamento na prateleira de armazenamento.
Slots de unidade	O número total de slots de unidade na prateleira de armazenamento.
Unidades de dados	O número de unidades na prateleira de armazenamento que são usadas para armazenamento de dados.
Tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados na prateleira de armazenamento.
Unidades de cache	O número de unidades na prateleira de armazenamento que são usadas como cache.
Tamanho da unidade de cache	O tamanho da menor unidade de cache na prateleira de armazenamento. Normalmente, todas as unidades de cache têm o mesmo tamanho.
Status da configuração	O status de configuração da prateleira de armazenamento.

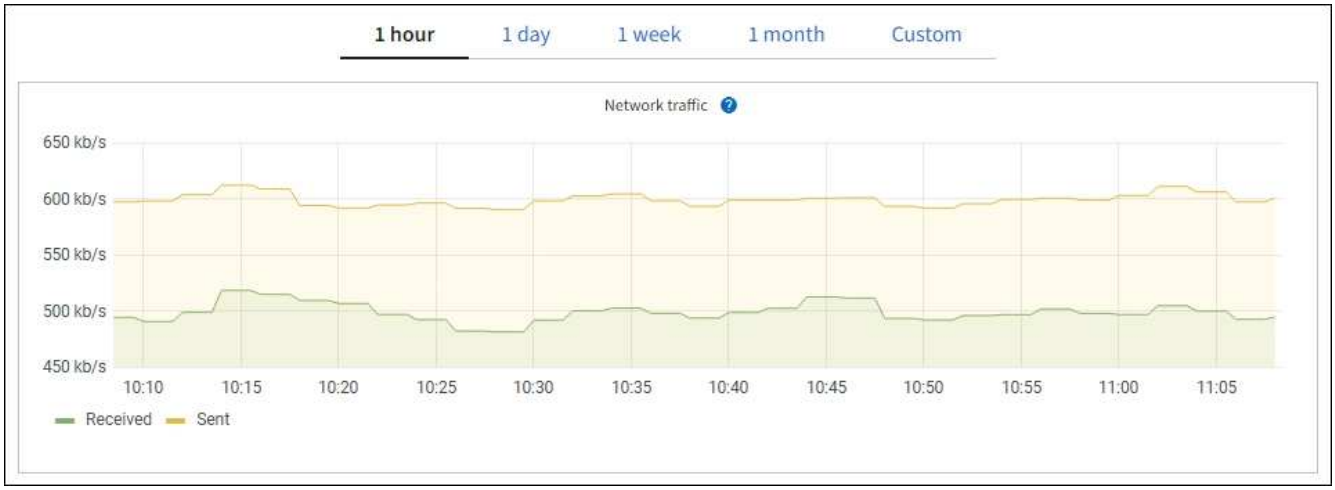
a. Confirme se todos os status são "Nominais".

   Se um status não for "Nominal", revise todos os alertas atuais. Você também pode usar o SANtricity System Manager para saber mais sobre alguns desses valores de hardware. Consulte as instruções

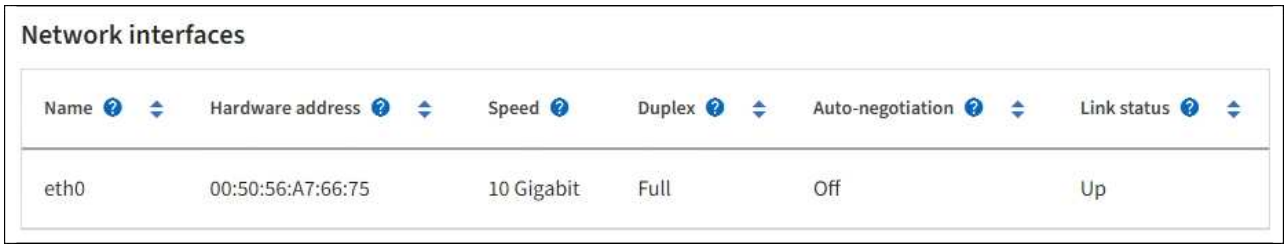
de instalação e manutenção do seu aparelho.

4. Selecione **Rede** para visualizar informações de cada rede.

   O gráfico Tráfego de rede fornece um resumo do tráfego geral da rede.



   a. Revise a seção Interfaces de rede.



   Use a tabela a seguir com os valores na coluna **Velocidade** na tabela Interfaces de rede para determinar se as portas de rede 10/25 GbE no dispositivo foram configuradas para usar o modo ativo/de backup ou o modo LACP.

   Os valores mostrados na tabela pressupõem que todos os quatro links sejam usados.

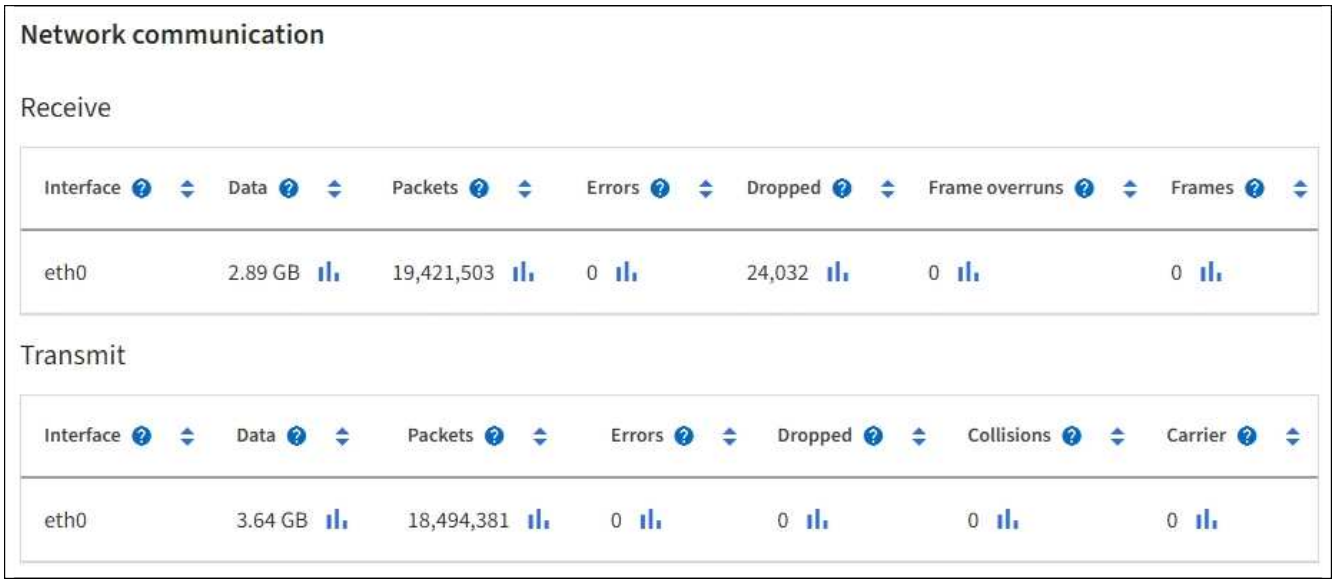
Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0,eth2)
Agregar	LACP	25	100
Fixo	LACP	25	50
Fixo	Ativo/Backup	25	25
Agregar	LACP	10	40
Fixo	LACP	10	20

Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0,eth2)
Fixo	Ativo/Backup	10	10

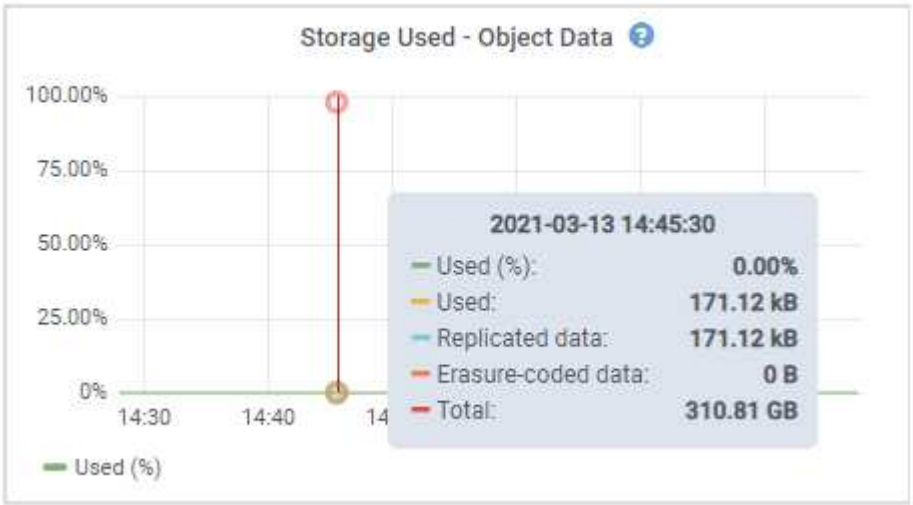
Ver "Configurar links de rede" para obter mais informações sobre como configurar as portas 10/25-GbE.

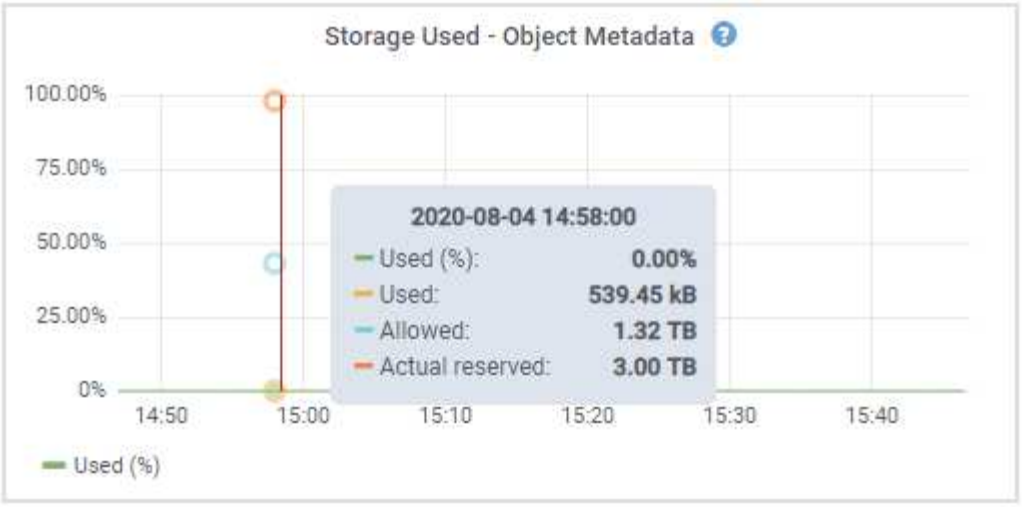
b. Revise a seção Comunicação de rede.

As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.



5. Selecione **Armazenamento** para visualizar gráficos que mostram as porcentagens de armazenamento usadas ao longo do tempo para dados de objetos e metadados de objetos, bem como informações sobre dispositivos de disco, volumes e armazenamentos de objetos.

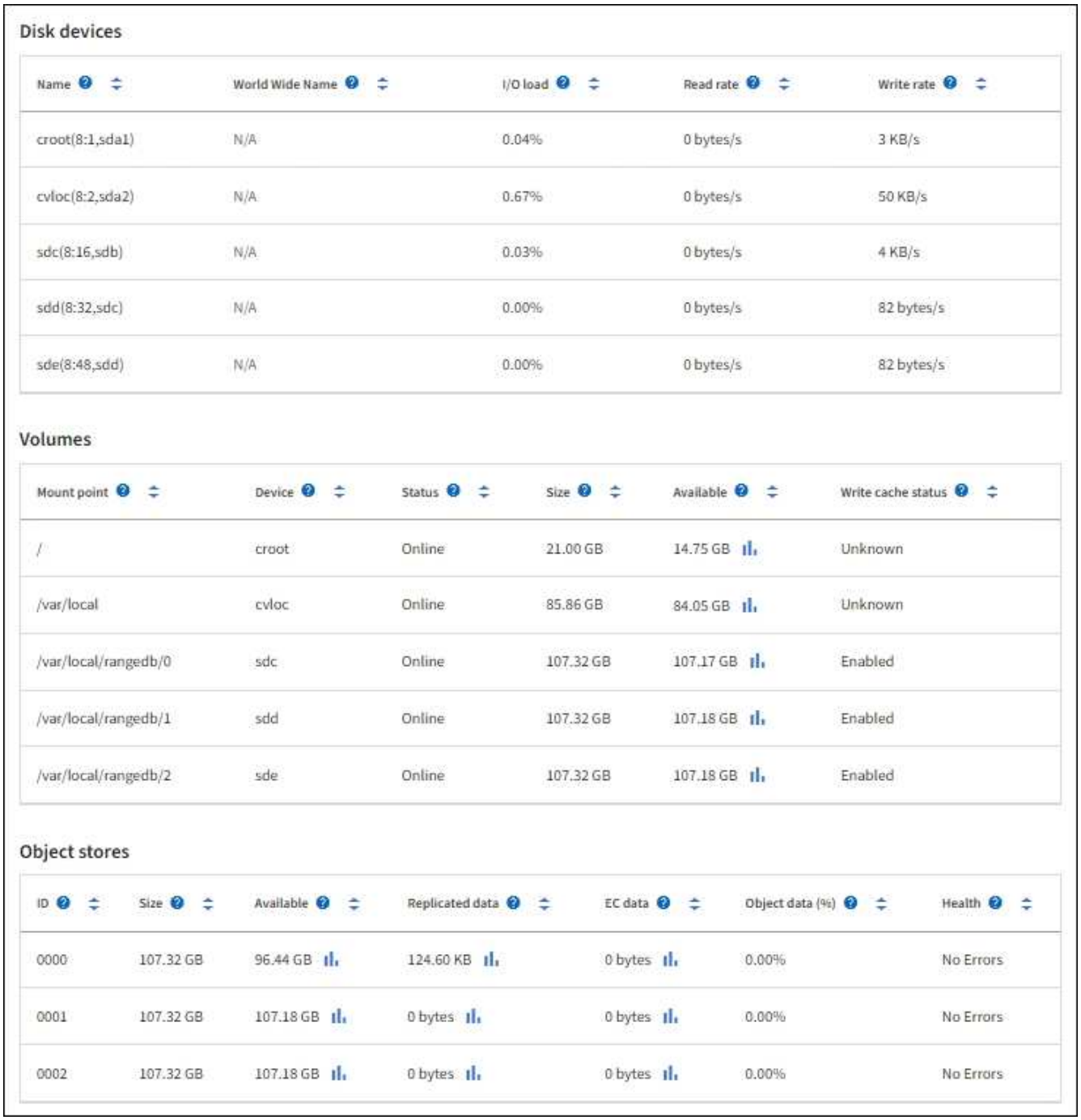




a. Role para baixo para ver as quantidades de armazenamento disponíveis para cada volume e armazenamento de objetos.

   O Nome Mundial de cada disco corresponde ao identificador mundial do volume (WWID) que aparece quando você visualiza as propriedades de volume padrão no SANtricity OS (o software de gerenciamento conectado ao controlador de armazenamento do dispositivo).

   Para ajudar você a interpretar estatísticas de leitura e gravação de disco relacionadas aos pontos de montagem de volume, a primeira parte do nome mostrada na coluna **Nome** da tabela Dispositivos de disco (ou seja, *sdc*, *sdd*, *sde* e assim por diante) corresponde ao valor mostrado na coluna **Dispositivo** da tabela Volumes.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Exibir informações sobre nós de administração e nós de gateway do dispositivo

A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada dispositivo de serviço usado como um Nó de administração ou um Nó de gateway. Você também pode ver memória, hardware de armazenamento, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

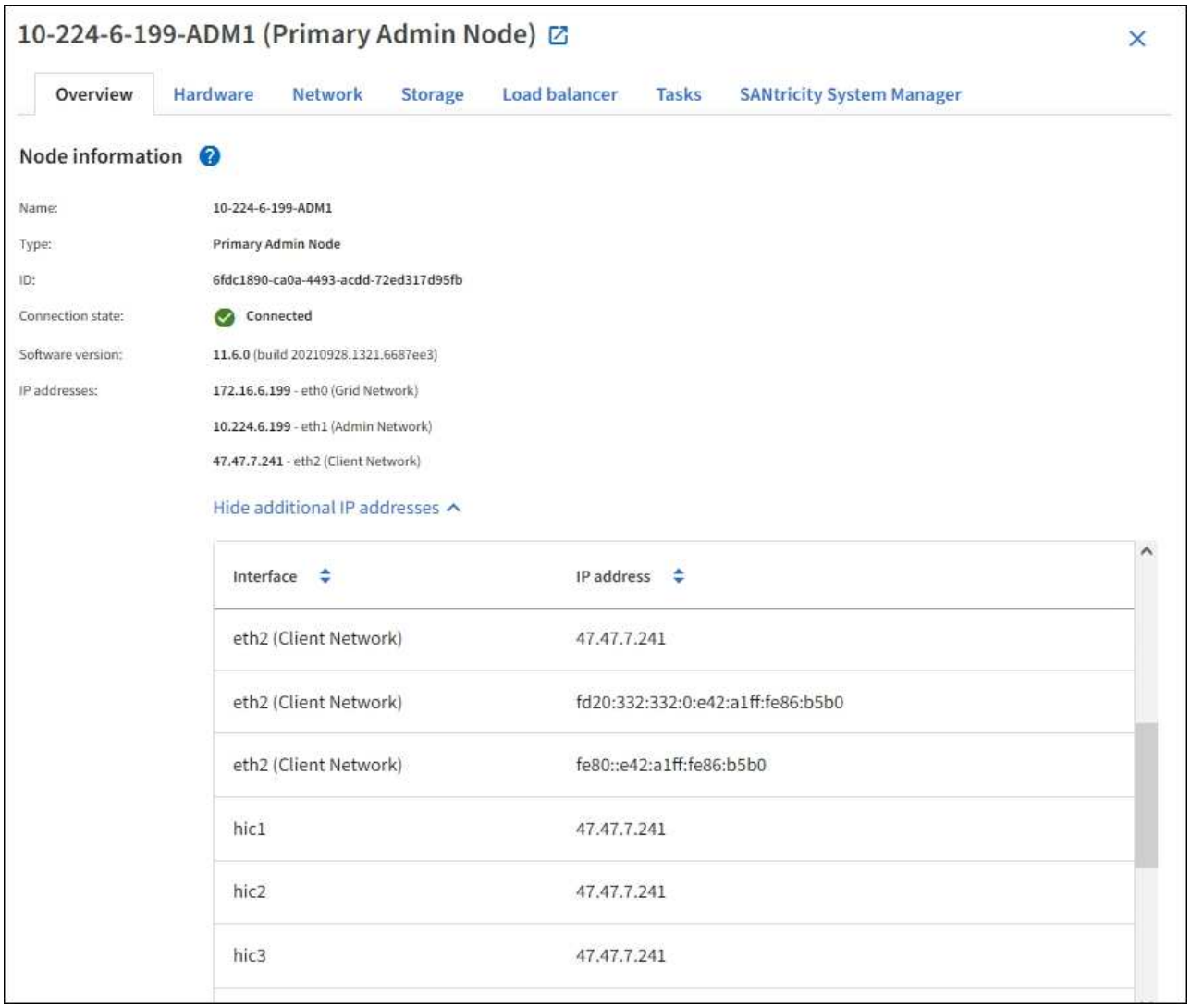
Passos

1. Na página Nós, selecione um Nó de administração do dispositivo ou um Nó de gateway do dispositivo.
2. Selecione **Visão geral**.

   A seção Informações do nó da guia Visão geral exibe informações resumidas do nó, como nome, tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte

forma:

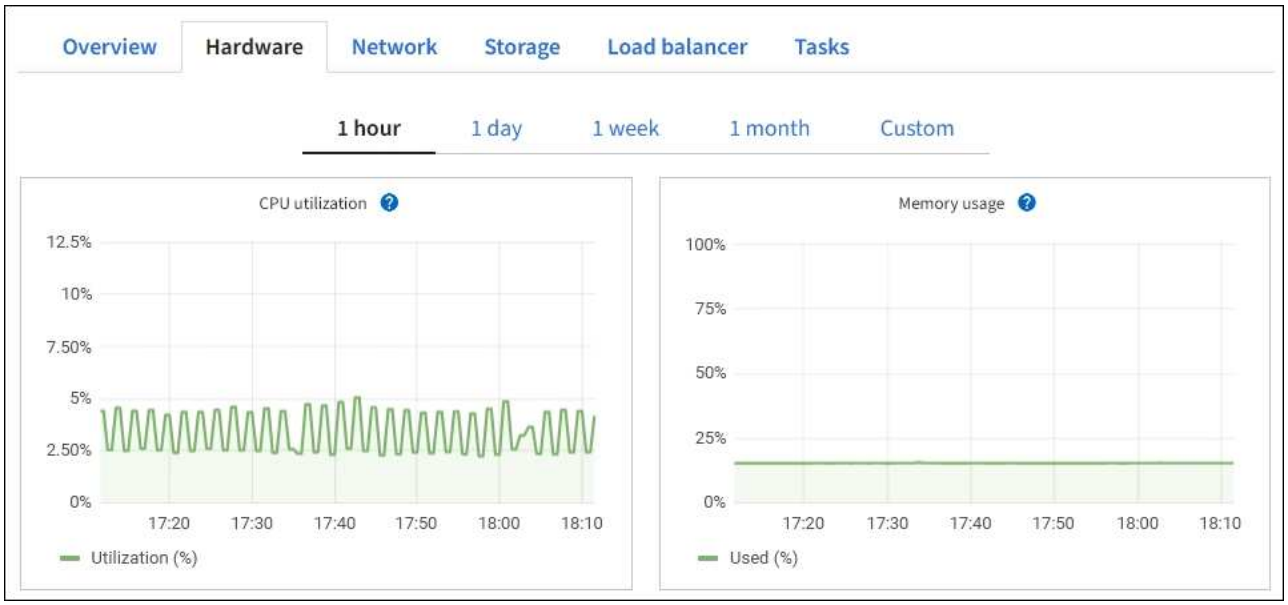
- **adllb** e **adlli**: Mostrados se a vinculação ativa/de backup for usada para a interface de rede de administração
- **eth**: Rede Grid, Rede Admin ou Rede Cliente.
- **soluço**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Essas portas podem ser vinculadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
- **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são vinculadas para formar a interface de rede de administração (eth1). Você pode deixar outras interfaces mtc disponíveis para conectividade local temporária para um técnico no data center.



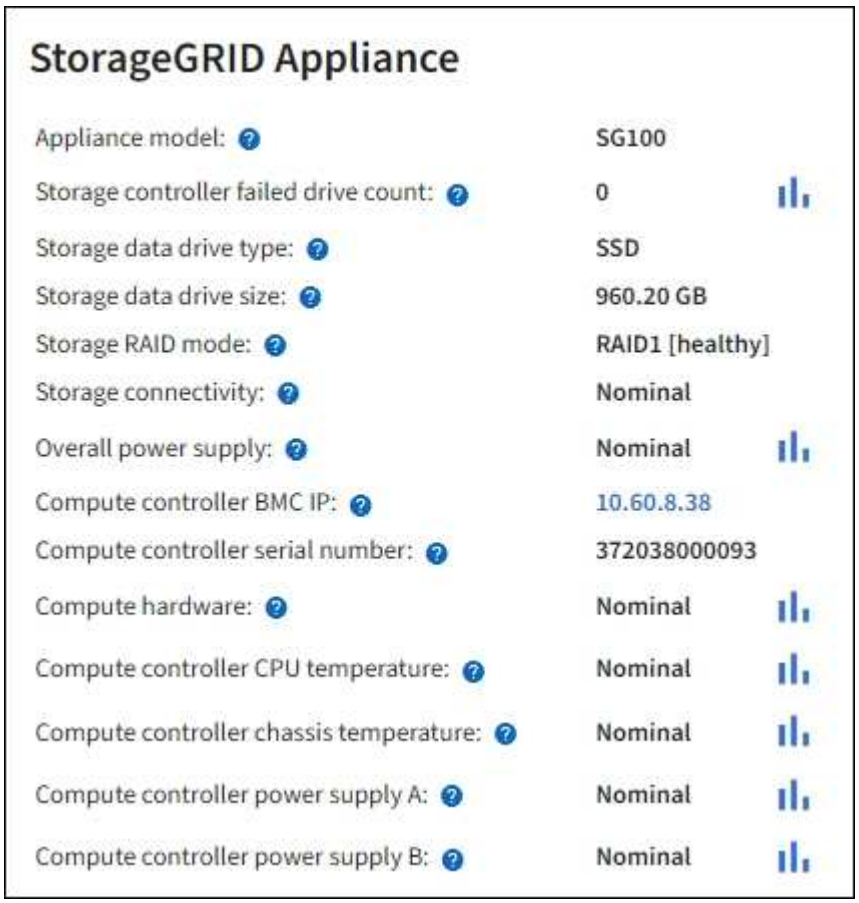
A seção Alertas da guia Visão geral exibe todos os alertas ativos para o nó.

3. Selecione **Hardware** para ver mais informações sobre o aparelho.

   a. Visualize os gráficos de Utilização da CPU e Memória para determinar as porcentagens de uso da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.



b. Role para baixo para ver a tabela de componentes do aparelho. Esta tabela contém informações como nome do modelo, número de série, versão do firmware do controlador e o status de cada componente.



Campo na tabela Appliance	Descrição
Modelo do aparelho	O número do modelo deste dispositivo StorageGRID .

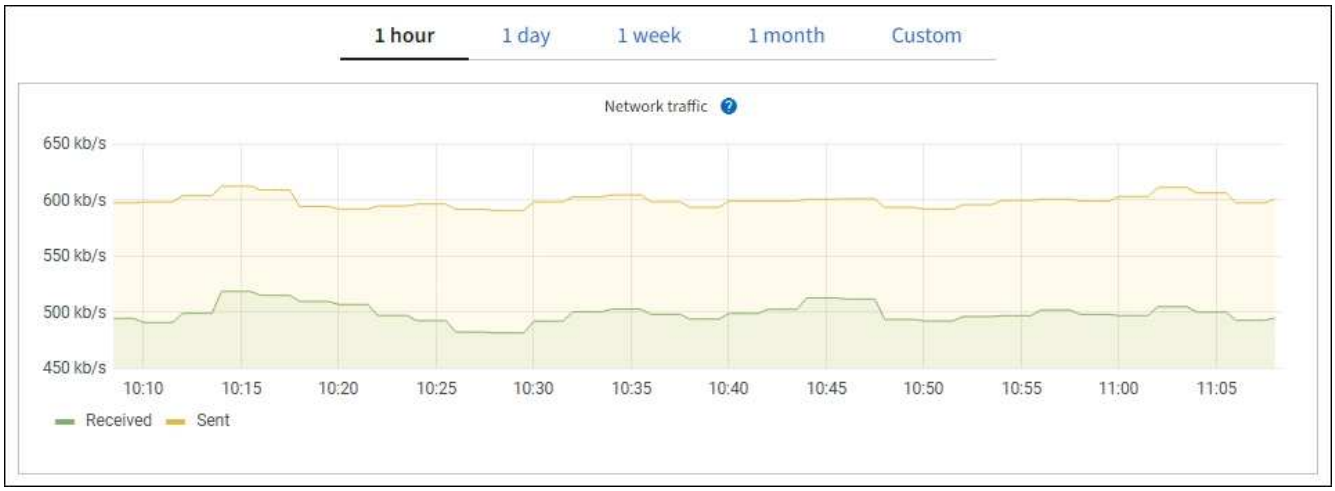
Campo na tabela Appliance	Descrição
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não são ideais.
Tipo de unidade de armazenamento de dados	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados.
Modo RAID de armazenamento	O modo RAID do dispositivo.
Fonte de alimentação geral	O status de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento da placa base (BMC) no controlador de computação. Você pode usar esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é exibido para modelos de aparelhos que não contêm um BMC.
Calcular o número de série do controlador	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação.
Controlador de computação de temperatura da CPU	O status da temperatura da CPU do controlador de computação.
Calcular a temperatura do chassi do controlador	O status da temperatura do controlador de computação.

a. Confirme se todos os status são "Nominais".

   Se um status não for "Nominal", revise todos os alertas atuais.

4. Selecione **Rede** para visualizar informações de cada rede.

   O gráfico Tráfego de rede fornece um resumo do tráfego geral da rede.



a. Revise a seção Interfaces de rede.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

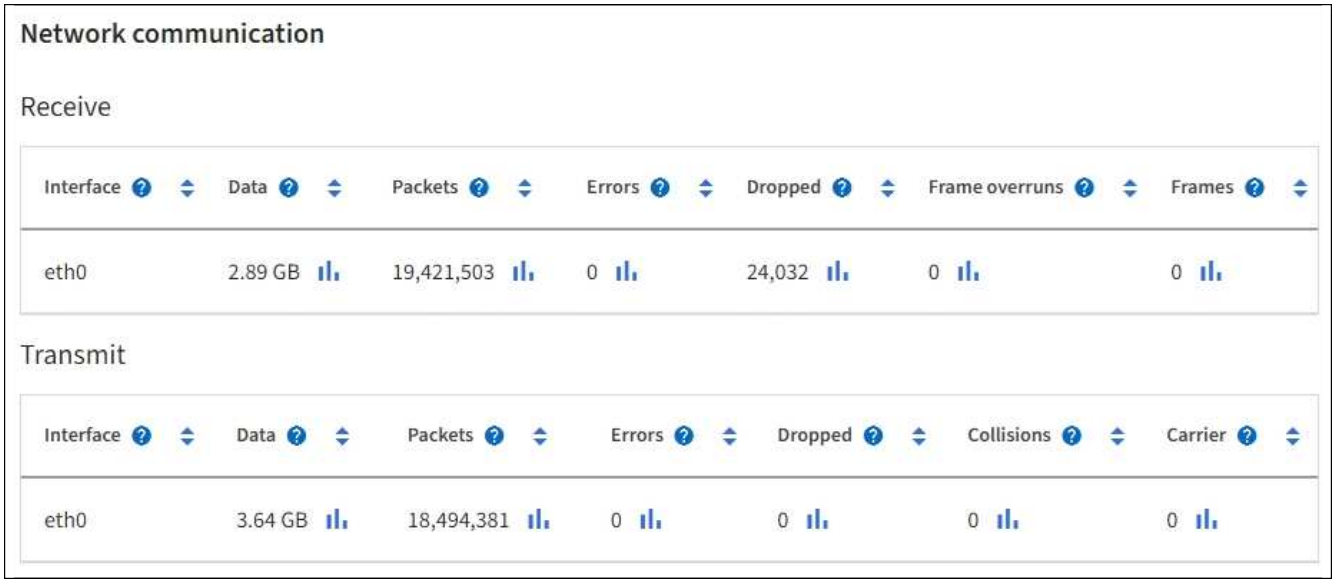
Use a tabela a seguir com os valores na coluna **Velocidade** na tabela Interfaces de rede para determinar se as quatro portas de rede 40/100 GbE no dispositivo foram configuradas para usar o modo ativo/de backup ou o modo LACP.

Os valores mostrados na tabela pressupõem que todos os quatro links sejam usados.

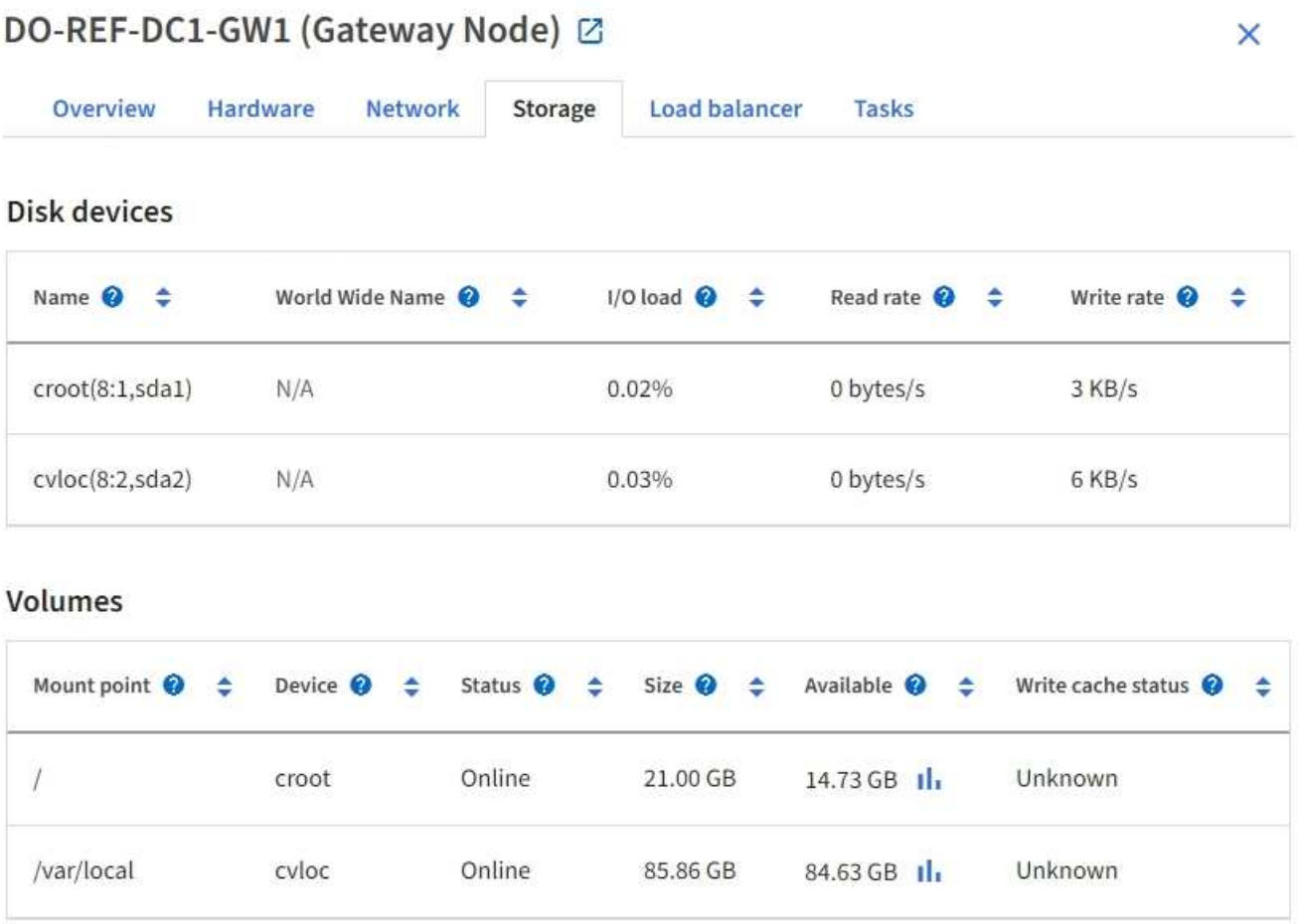
Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0, eth2)
Agregar	LACP	100	400
Fixo	LACP	100	200
Fixo	Ativo/Backup	100	100
Agregar	LACP	40	160
Fixo	LACP	40	80
Fixo	Ativo/Backup	40	40

b. Revise a seção Comunicação de rede.

As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.



5. Selecione **Armazenamento** para visualizar informações sobre os dispositivos de disco e volumes no dispositivo de serviços.



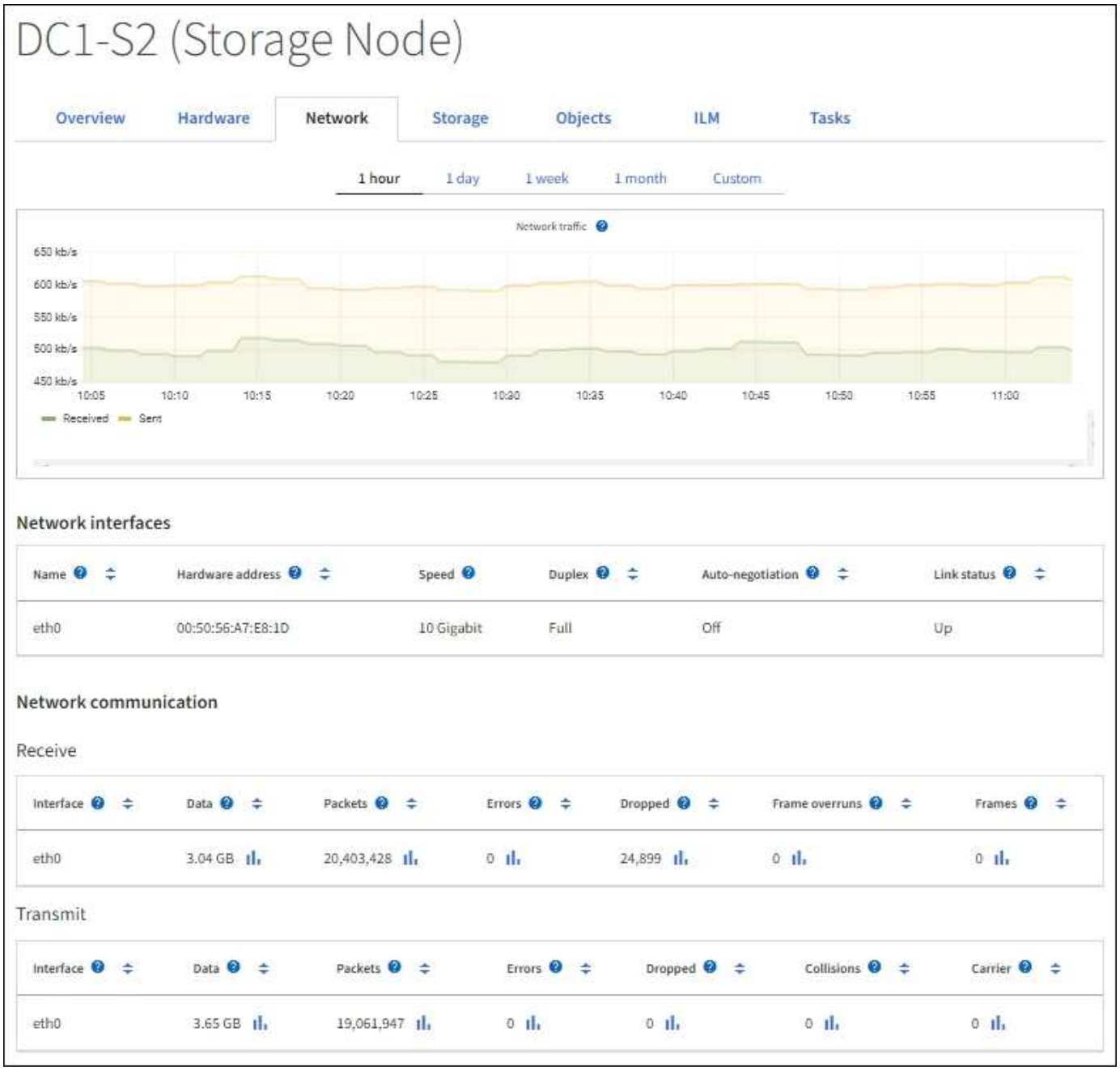
Ver a aba Rede

A guia Rede exibe um gráfico mostrando o tráfego de rede recebido e enviado por todas as interfaces de rede no nó, site ou grade.

A guia Rede é exibida para todos os nós, cada site e toda a grade.

Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.

Para nós, a tabela Interfaces de rede fornece informações sobre as portas de rede física de cada nó. A tabela de comunicações de rede fornece detalhes sobre as operações de recepção e transmissão de cada nó e quaisquer contadores de falhas relatados pelo driver.



Informações relacionadas

"Monitore as conexões e o desempenho da rede"

Ver a aba Armazenamento

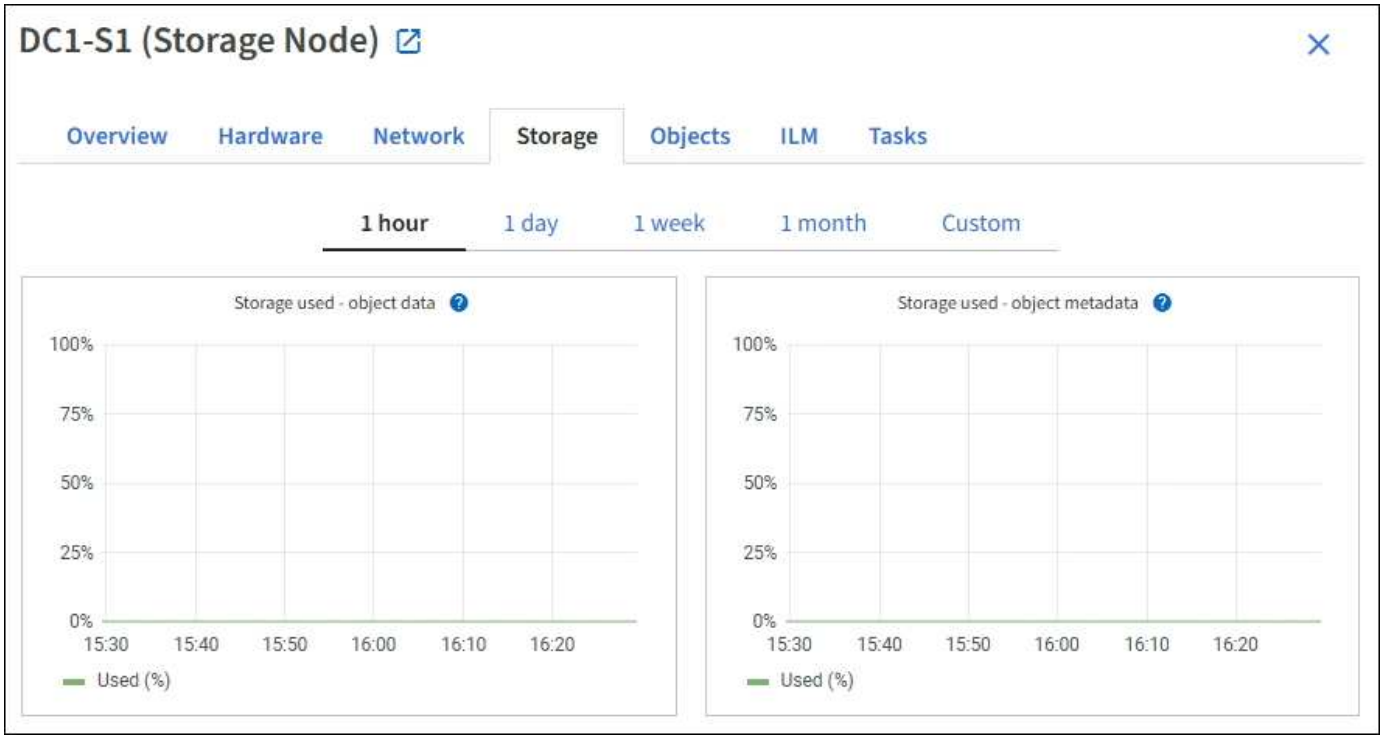
A guia Armazenamento resume a disponibilidade de armazenamento e outras métricas de armazenamento.

A guia Armazenamento é exibida para todos os nós, cada site e toda a grade.

Gráficos de armazenamento usados

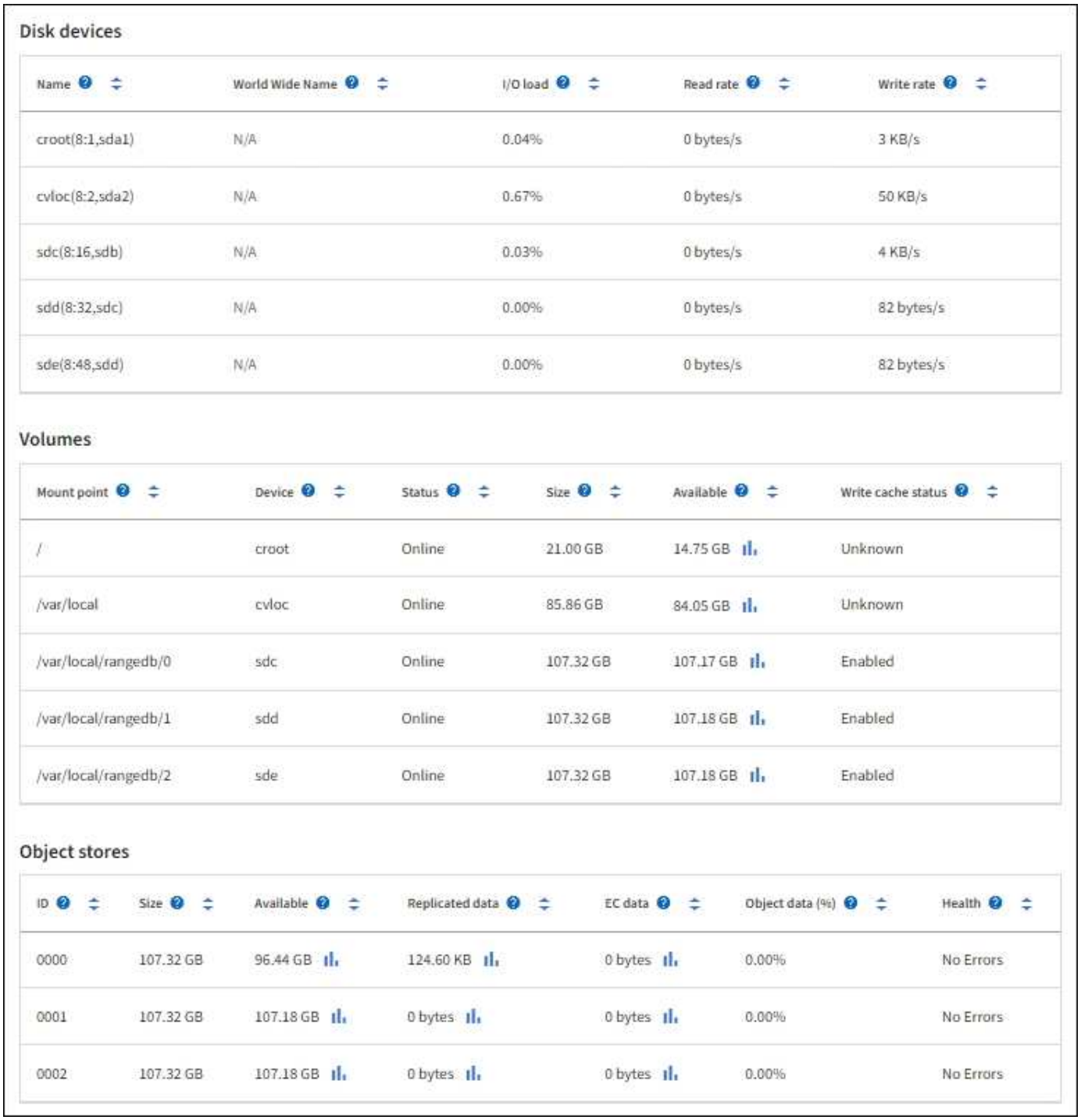
Para nós de armazenamento, cada site e toda a grade, a guia Armazenamento inclui gráficos que mostram quanto armazenamento foi usado por dados de objeto e metadados de objeto ao longo do tempo.

Quando um nó não está conectado à rede, como durante uma atualização ou em um estado desconectado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da rede. Depois que um nó se reconectar à rede, aguarde alguns minutos para que os valores se estabilizem.



Dispositivos de disco, volumes e tabelas de armazenamento de objetos

Para todos os nós, a guia Armazenamento contém detalhes dos dispositivos de disco e volumes no nó. Para nós de armazenamento, a tabela Object Stores fornece informações sobre cada volume de armazenamento.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

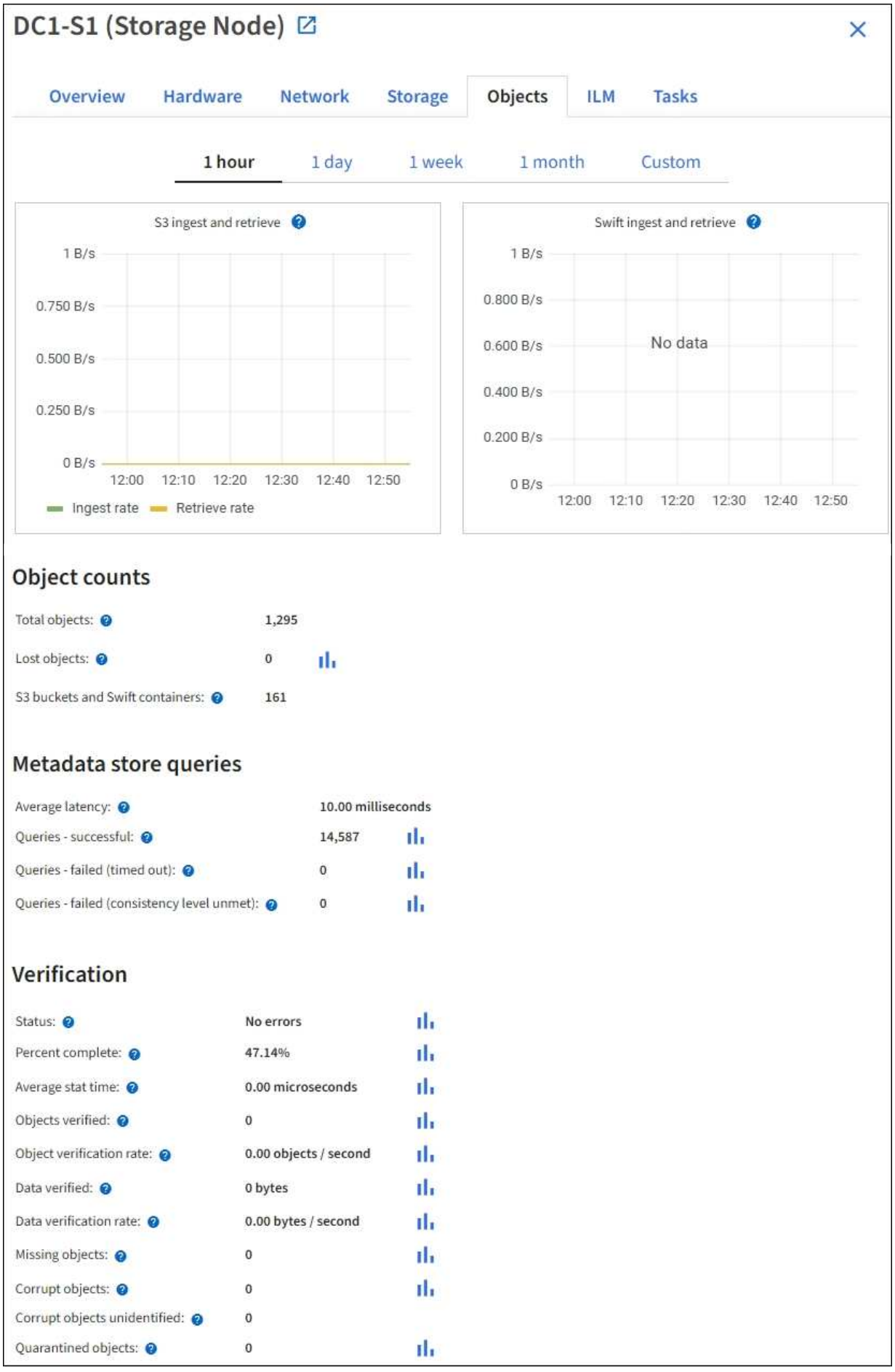
Informações relacionadas

"Monitorar capacidade de armazenamento"

Ver a aba Objetos

A guia Objetos fornece informações sobre"Taxas de ingestão e recuperação do S3" .

A guia Objetos é exibida para cada nó de armazenamento, cada site e toda a grade. Para nós de armazenamento, a guia Objetos também fornece contagens de objetos e informações sobre consultas de metadados e verificação de antecedentes.

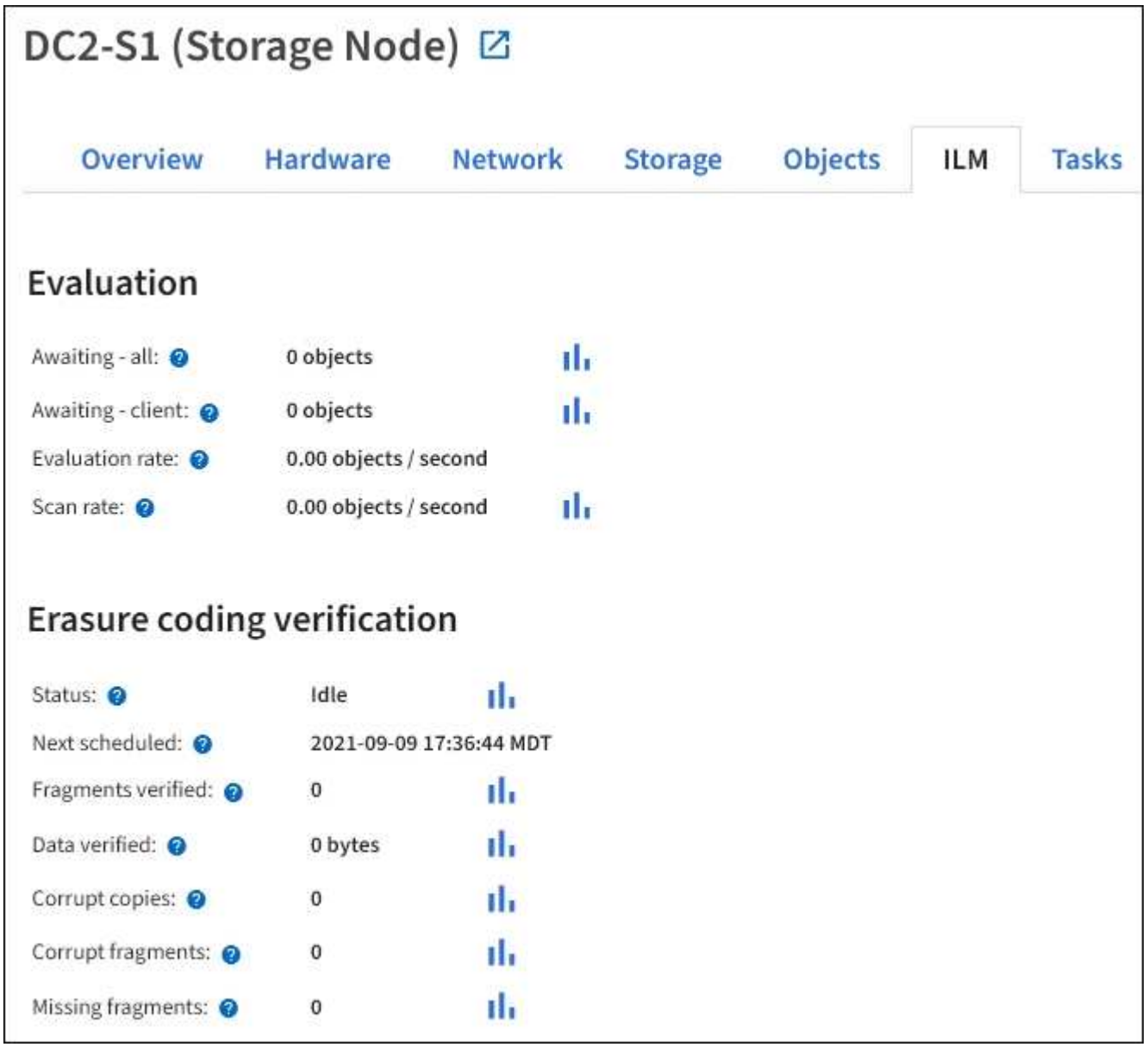

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Ver a aba ILM

A guia ILM fornece informações sobre operações de gerenciamento do ciclo de vida das informações (ILM).

A guia ILM é exibida para cada nó de armazenamento, cada site e toda a grade. Para cada site e grade, a guia ILM mostra um gráfico da fila do ILM ao longo do tempo. Para a grade, esta guia também fornece o tempo estimado para concluir uma varredura ILM completa de todos os objetos.

Para nós de armazenamento, a guia ILM fornece detalhes sobre a avaliação do ILM e a verificação em segundo plano para objetos codificados para eliminação.



Informações relacionadas

- "Monitorar o gerenciamento do ciclo de vida das informações"
- "Administrar StorageGRID"

Use a aba Tarefas

A guia Tarefas é exibida para todos os nós. Você pode usar esta guia para renomear ou reinicializar um nó ou colocar um nó do dispositivo no modo de manutenção.

Para obter os requisitos e instruções completos para cada opção nesta guia, consulte o seguinte:

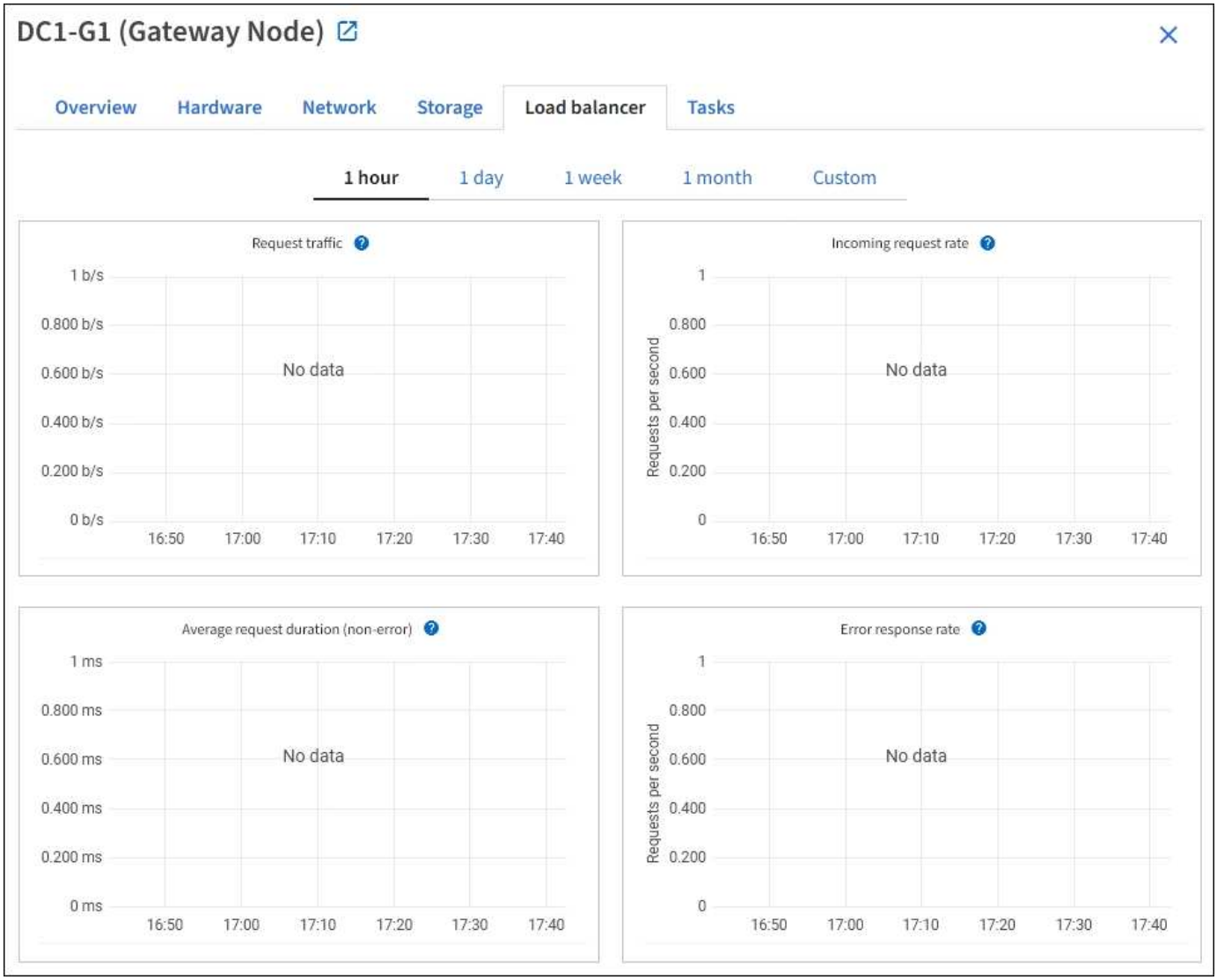
- "Renomear grade, sites e nós"
- "Reinicializar nó de grade"
- "Coloque o aparelho em modo de manutenção"

Exibir a guia Balanceador de carga

A guia Balanceador de Carga inclui gráficos de desempenho e diagnóstico relacionados à operação do serviço Balanceador de Carga.

A guia Balanceador de Carga é exibida para Nós de Administração e Nós de Gateway, cada site e toda a grade. Para cada site, a guia Balanceador de Carga fornece um resumo agregado das estatísticas de todos os nós naquele site. Para toda a grade, a guia Balanceador de Carga fornece um resumo agregado das estatísticas de todos os sites.

Se não houver E/S sendo executada pelo serviço Load Balancer, ou se não houver nenhum balanceador de carga configurado, os gráficos exibirão "Nenhum dado".



Solicitar tráfego

Este gráfico fornece uma média móvel de 3 minutos da taxa de transferência de dados transmitidos entre os pontos de extremidade do balanceador de carga e os clientes que fazem as solicitações, em bits por segundo.

> Este valor é atualizado na conclusão de cada solicitação. Como resultado, esse valor pode ser diferente da taxa de transferência em tempo real em taxas de solicitação baixas ou para solicitações de duração muito longa. Você pode consultar a aba Rede para ter uma visão mais realista do comportamento atual da rede.

Taxa de solicitação de entrada

Este gráfico fornece uma média móvel de 3 minutos do número de novas solicitações por segundo, divididas por tipo de solicitação (GET, PUT, HEAD e DELETE). Este valor é atualizado quando os cabeçalhos de uma nova solicitação são validados.

Duração média da solicitação (sem erro)

Este gráfico fornece uma média móvel de 3 minutos de durações de solicitações, divididas por tipo de solicitação (GET, PUT, HEAD e DELETE). Cada duração de solicitação começa quando um cabeçalho de solicitação é analisado pelo serviço Load Balancer e termina quando o corpo de resposta completo é

retornado ao cliente.

Taxa de resposta de erro

Este gráfico fornece uma média móvel de 3 minutos do número de respostas de erro retornadas aos clientes por segundo, divididas pelo código de resposta de erro.

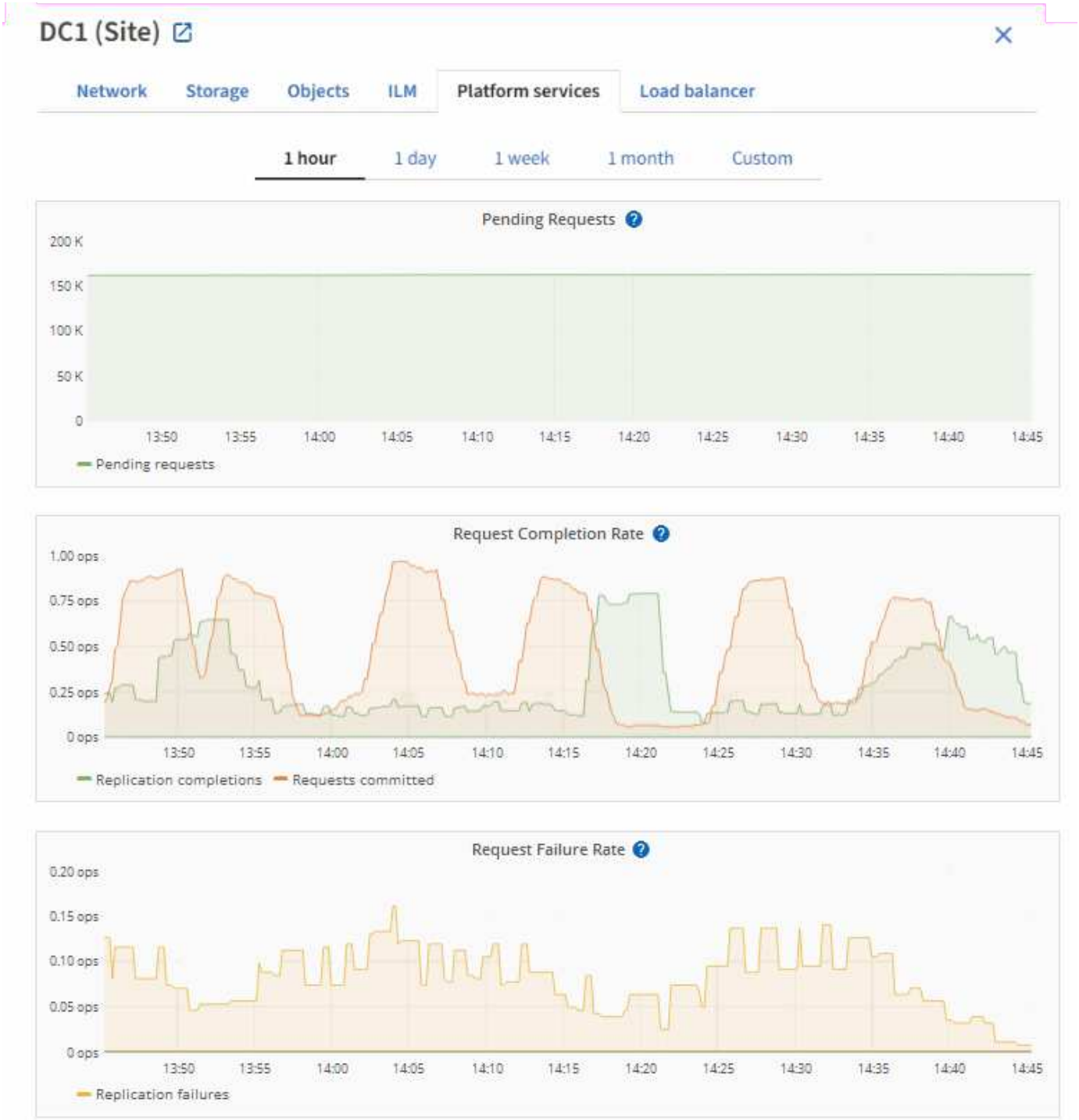
Informações relacionadas

- "Monitorar operações de balanceamento de carga"
- "Administrar StorageGRID"

Ver a aba Serviços da plataforma

A guia Serviços da plataforma fornece informações sobre quaisquer operações de serviço da plataforma S3 em um site.

A aba Serviços da plataforma é exibida para cada site. Esta guia fornece informações sobre os serviços da plataforma S3, como a replicação do CloudMirror e o serviço de integração de pesquisa. Os gráficos nesta guia exibem métricas como o número de solicitações pendentes, a taxa de conclusão da solicitação e a taxa de falha da solicitação.



Para obter mais informações sobre os serviços da plataforma S3, incluindo detalhes de solução de problemas, consulte o"instruções para administrar o StorageGRID" .

Exibir a guia Gerenciar unidades

A guia Gerenciar unidades permite que você acesse detalhes e execute tarefas de solução de problemas e manutenção em unidades nos dispositivos que oferecem suporte a esse recurso.

Usando a guia Gerenciar unidades, você pode fazer o seguinte:

- Visualize um layout das unidades de armazenamento de dados no dispositivo
- Veja uma tabela que lista cada local da unidade, tipo, status, versão do firmware e número de série
- Executar funções de solução de problemas e manutenção em cada unidade

Para acessar a aba Gerenciar unidades, você deve ter o"Permissão de acesso root ou de administrador do dispositivo de armazenamento" .

Para obter informações sobre como usar a guia Gerenciar unidades, consulte "Use a guia Gerenciar unidades" .

Exibir a guia SANtricity System Manager (somente Série E)

A guia SANtricity System Manager permite que você acesse o SANtricity System Manager sem precisar configurar ou conectar a porta de gerenciamento do dispositivo de armazenamento. Você pode usar esta guia para revisar diagnósticos de hardware e informações ambientais, bem como problemas relacionados às unidades.

> O acesso ao SANtricity System Manager a partir do Grid Manager geralmente serve apenas para monitorar o hardware do dispositivo e configurar o E-Series AutoSupport. Muitos recursos e operações do SANtricity System Manager, como atualização de firmware, não se aplicam ao monitoramento do seu dispositivo StorageGRID . Para evitar problemas, siga sempre as instruções de manutenção de hardware do seu aparelho. Para atualizar o firmware do SANtricity , consulte o "Procedimentos de configuração de manutenção" para seu dispositivo de armazenamento.

> A guia SANtricity System Manager é exibida somente para nós de dispositivos de armazenamento que usam hardware da Série E.

Usando o SANtricity System Manager, você pode fazer o seguinte:

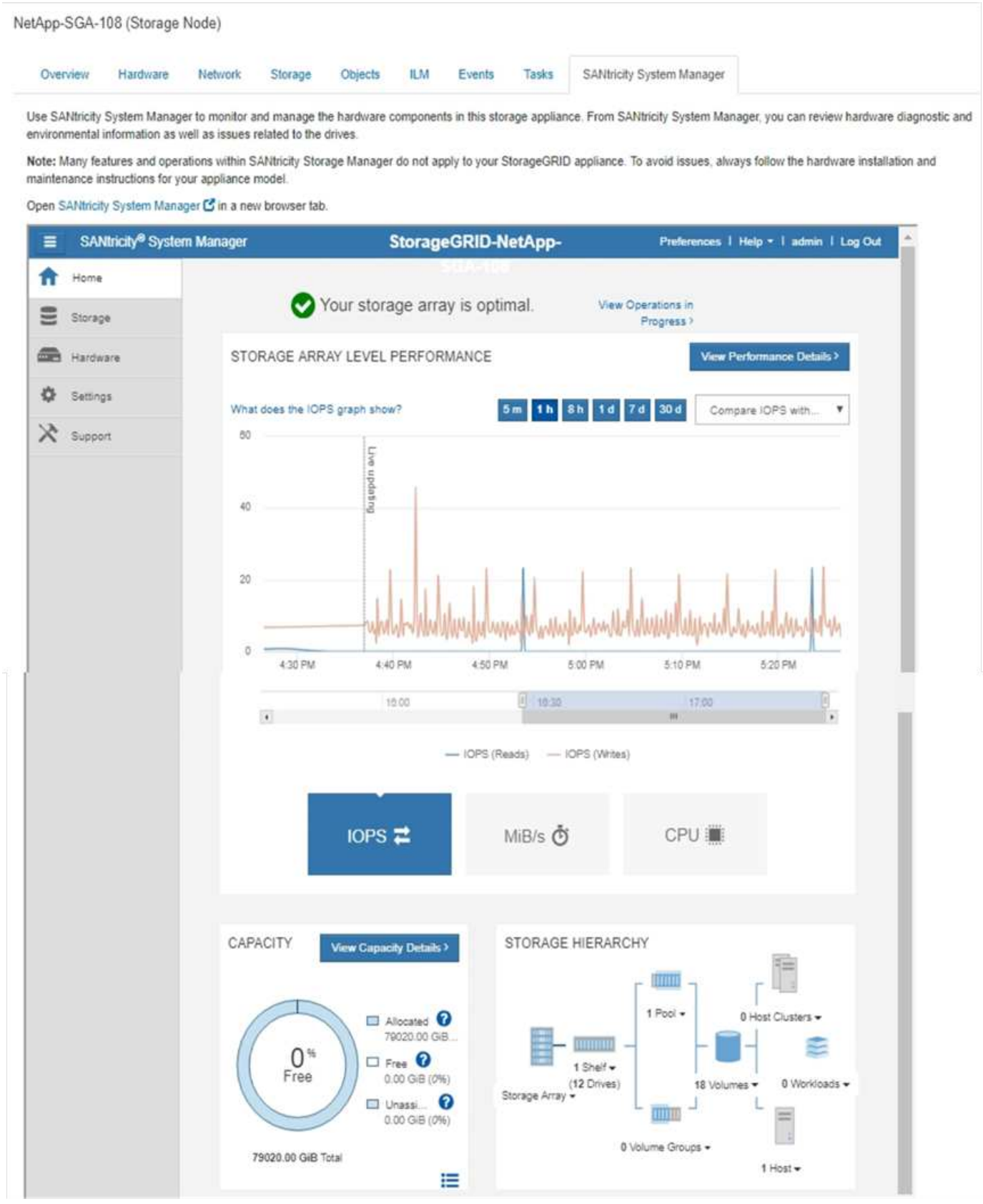
- Visualize dados de desempenho, como desempenho em nível de matriz de armazenamento, latência de E/S, utilização de CPU do controlador de armazenamento e taxa de transferência.
- Verifique o status do componente de hardware.
- Execute funções de suporte, incluindo visualização de dados de diagnóstico e configuração do E-Series AutoSupport.

> Para usar o SANtricity System Manager para configurar um proxy para o E-Series AutoSupport, consulte"Enviar pacotes E-Series AutoSupport por meio do StorageGRID" .

Para acessar o SANtricity System Manager por meio do Grid Manager, você deve ter o"Permissão de acesso root ou de administrador do dispositivo de armazenamento" .

> Você deve ter o firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

A guia exibe a página inicial do SANtricity System Manager.



Você pode usar o link do SANtricity System Manager para abrir o SANtricity System Manager em uma nova janela do navegador para facilitar a visualização.

Para ver detalhes sobre o desempenho do nível de matriz de armazenamento e o uso da capacidade,

posicione o cursor sobre cada gráfico.

Para obter mais detalhes sobre como visualizar as informações acessíveis na guia SANtricity System Manager, consulte "Documentação do NetApp E-Series e SANtricity" .

Informações para monitorar regularmente

O que e quando monitorar

Mesmo que o sistema StorageGRID possa continuar a operar quando ocorrerem erros ou partes da rede estiverem indisponíveis, você deve monitorar e resolver possíveis problemas antes que eles afetem a eficiência ou a disponibilidade da rede.

Antes de começar

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

Sobre tarefas de monitoramento

Um sistema ocupado gera grandes quantidades de informações. A lista a seguir fornece orientação sobre as informações mais importantes a serem monitoradas continuamente.

O que monitorar	Freqüência
"Status de saúde do sistema"	Diário
Taxa na qual"Capacidade de objetos e metadados do nó de armazenamento" está sendo consumido	Semanalmente
"Operações de gerenciamento do ciclo de vida da informação"	Semanalmente
"Recursos de rede e sistema"	Semanalmente
"Atividade do inquilino"	Semanalmente
"Operações do cliente S3"	Semanalmente
"Operações de balanceamento de carga"	Após a configuração inicial e após quaisquer alterações de configuração
"Conexões de federação de rede"	Semanalmente

Monitorar a saúde do sistema

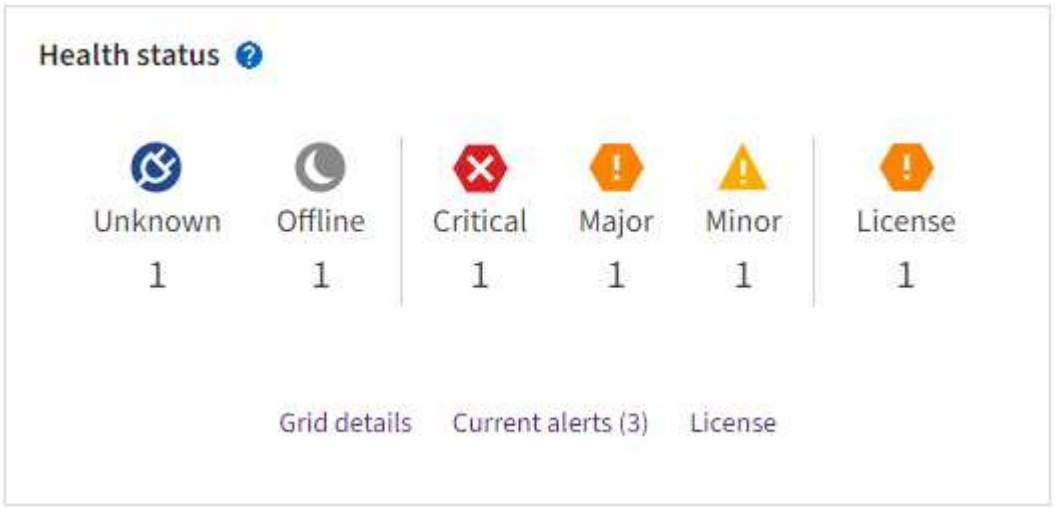
Monitore a saúde geral do seu sistema StorageGRID diariamente.

Sobre esta tarefa

O sistema StorageGRID pode continuar a operar quando partes da rede não estiverem disponíveis. Possíveis problemas indicados por alertas não são necessariamente problemas com operações do sistema. Investigue

os problemas resumidos no cartão de status de integridade do painel do Grid Manager.

Para ser notificado sobre alertas assim que eles forem acionados, você pode "configurar notificações por e-mail para alertas" ou"configurar armadilhas SNMP" .



Quando há problemas, aparecem links que permitem visualizar detalhes adicionais:

Link	Aparece quando…
Detalhes da grade	Todos os nós estão desconectados (estado de conexão Desconhecido ou Administrativamente Inativo).
Alertas atuais (crítico, grave, secundário)	Os alertas sãoatualmente ativo .
Alertas resolvidos recentemente	Alertas acionados na semana passadaagora estão resolvidos .
Licença	Há um problema com a licença de software para este sistema StorageGRID . Você pode "atualizar informações de licença conforme necessário" .

Monitorar estados de conexão de nós

Se um ou mais nós forem desconectados da grade, operações críticas do StorageGRID poderão ser afetadas. Monitore os estados de conexão dos nós e resolva quaisquer problemas imediatamente.

Ícone	Descrição	Ação necessária
	Não conectado - Desconhecido Por um motivo desconhecido, um nó é desconectado ou os serviços no nó ficam inesperadamente inativos. Por exemplo, um serviço no nó pode ser interrompido, ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta **Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. Selecione cada alerta e siga as ações recomendadas. Por exemplo, talvez seja necessário reiniciar um serviço que foi interrompido ou reiniciar o host do nó. **Observação**: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	Não conectado - Inativo administrativamente Por um motivo esperado, o nó não está conectado à rede. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Determine se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos,selecione cada alerta e siga as ações recomendadas.
	Conectado O nó está conectado à rede.	Nenhuma ação necessária.

Ver alertas atuais e resolvidos

Alertas atuais: Quando um alerta é acionado, um ícone de alerta é exibido no painel. Um ícone de alerta também é exibido para o nó na página Nós. Se"notificações de alerta por e-mail são configuradas" , uma notificação por e-mail também será enviada, a menos que o alerta tenha sido silenciado.

Alertas resolvidos: Você pode pesquisar e visualizar um histórico de alertas que foram resolvidos.

Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral dos alertas"

A tabela a seguir descreve as informações mostradas no Grid Manager para alertas atuais e resolvidos.

Cabeçalho da coluna	Descrição
Nome ou título	O nome do alerta e sua descrição.
Gravidade	A gravidade do alerta. Para alertas atuais, se vários alertas forem agrupados, a linha de título mostrará quantas instâncias desse alerta estão ocorrendo em cada gravidade. **Crítico**: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido. **Principal**: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID . **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.
Tempo acionado	**Alertas atuais**: A data e a hora em que o alerta foi disparado no seu horário local e em UTC. Se vários alertas forem agrupados, a linha de título mostrará os horários da instância mais recente do alerta (*newest*) e da instância mais antiga do alerta (*oldest*). **Alertas resolvidos**: Há quanto tempo o alerta foi disparado.
Site/Nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.
Status	Se o alerta está ativo, silenciado ou resolvido. Se vários alertas forem agrupados e **Todos os alertas** for selecionado no menu suspenso, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.

Cabeçalho da coluna	Descrição
Tempo resolvido (somente alertas resolvidos)	Há quanto tempo o alerta foi resolvido.
Valores atuais ou *valores de dados*	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, valores adicionais são mostrados para ajudar você a entender e investigar o alerta. Por exemplo, os valores mostrados para um alerta de **Armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado. **Observação:** Se vários alertas atuais forem agrupados, os valores atuais não serão exibidos na linha de título.
Valores acionados (somente alertas resolvidos)	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, valores adicionais são mostrados para ajudar você a entender e investigar o alerta. Por exemplo, os valores mostrados para um alerta de **Armazenamento de dados de objeto baixo** incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

Passos

1. Selecione o link **Alertas atuais** ou **Alertas resolvidos** para visualizar uma lista de alertas nessas categorias. Você também pode visualizar os detalhes de um alerta selecionando **Nós** > ***nó*** > **Visão geral** e, em seguida, selecionando o alerta na tabela Alertas.

   Por padrão, os alertas atuais são mostrados da seguinte forma:

   - Os alertas disparados mais recentemente são mostrados primeiro.
   - Vários alertas do mesmo tipo são exibidos como um grupo.
   - Alertas que foram silenciados não são exibidos.
   - Para um alerta específico em um nó específico, se os limites forem atingidos para mais de uma gravidade, somente o alerta mais grave será mostrado. Ou seja, se os limites de alerta forem atingidos para as gravidades menor, maior e crítica, somente o alerta crítico será exibido.

     A página Alertas atuais é atualizada a cada dois minutos.

2. Para expandir grupos de alertas, selecione o cursor para baixo . Para recolher alertas individuais em um grupo, selecione o cursor para cima , ou selecione o nome do grupo.
3. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **Alertas de grupo**.
4. Para classificar alertas atuais ou grupos de alertas, selecione as setas para cima/baixo em cada cabeçalho de coluna.
   - Quando **Alertas de grupo** é selecionado, tanto os grupos de alertas quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **Tempo de acionamento** para encontrar a instância mais recente de um alerta específico.
   - Quando **Alertas de grupo** é limpo, toda a lista de alertas é classificada. Por exemplo, você pode querer classificar todos os alertas por **Nó/Site** para ver todos os alertas que afetam um nó específico.
5. Para filtrar alertas atuais por status (**Todos os alertas**, **Ativos** ou **Silenciados**, use o menu suspenso na

parte superior da tabela.

Ver "Silenciar notificações de alerta" .

6. Para classificar alertas resolvidos:
   - Selecione um período de tempo no menu suspenso **Quando acionado**.
   - Selecione uma ou mais gravidades no menu suspenso **Gravidade**.
   - Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **Regra de alerta** para filtrar alertas resolvidos relacionados a uma regra de alerta específica.
   - Selecione um ou mais nós no menu suspenso **Nó** para filtrar alertas resolvidos relacionados a um nó específico.
7. Para visualizar detalhes de um alerta específico, selecione o alerta. Uma caixa de diálogo fornece detalhes e ações recomendadas para o alerta selecionado.
8. (Opcional) Para um alerta específico, selecione silenciar este alerta para silenciar a regra de alerta que causou o disparo deste alerta.

   Você deve ter o"Gerenciar alertas ou permissão de acesso root" para silenciar uma regra de alerta.

   > Tenha cuidado ao decidir silenciar uma regra de alerta. Se uma regra de alerta for silenciada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

9. Para visualizar as condições atuais da regra de alerta:
   a. Nos detalhes do alerta, selecione **Exibir condições**.

      Um pop-up aparece, listando a expressão do Prometheus para cada gravidade definida.

   b. Para fechar o pop-up, clique em qualquer lugar fora dele.
10. Opcionalmente, selecione **Editar regra** para editar a regra de alerta que causou o disparo deste alerta.

    Você deve ter o"Gerenciar alertas ou permissão de acesso root" para editar uma regra de alerta.

    > Tenha cuidado ao decidir editar uma regra de alerta. Se você alterar os valores do gatilho, talvez não seja possível detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

11. Para fechar os detalhes do alerta, selecione **Fechar**.

Monitorar capacidade de armazenamento

Monitore o espaço total utilizável disponível para garantir que o sistema StorageGRID não fique sem espaço de armazenamento para objetos ou para metadados de objetos.

O StorageGRID armazena dados de objetos e metadados de objetos separadamente e reserva uma quantidade específica de espaço para um banco de dados Cassandra distribuído que contém metadados de objetos. Monitore a quantidade total de espaço consumido por objetos e metadados de objetos, bem como tendências na quantidade de espaço consumido por cada um. Isso permitirá que você planeje com antecedência a adição de nós e evite interrupções de serviço.

Você pode"ver informações sobre capacidade de armazenamento" para toda a grade, para cada site e para

cada nó de armazenamento no seu sistema StorageGRID .

Monitorar a capacidade de armazenamento de toda a rede

Monitore a capacidade geral de armazenamento da sua grade para garantir que haja espaço livre adequado para dados e metadados de objetos. Entender como a capacidade de armazenamento muda ao longo do tempo pode ajudar você a planejar a adição de nós de armazenamento ou volumes de armazenamento antes que a capacidade de armazenamento utilizável da grade seja consumida.

O painel do Grid Manager permite que você avalie rapidamente quanto armazenamento está disponível para toda a grade e para cada data center. A página Nós fornece valores mais detalhados para dados de objetos e metadados de objetos.

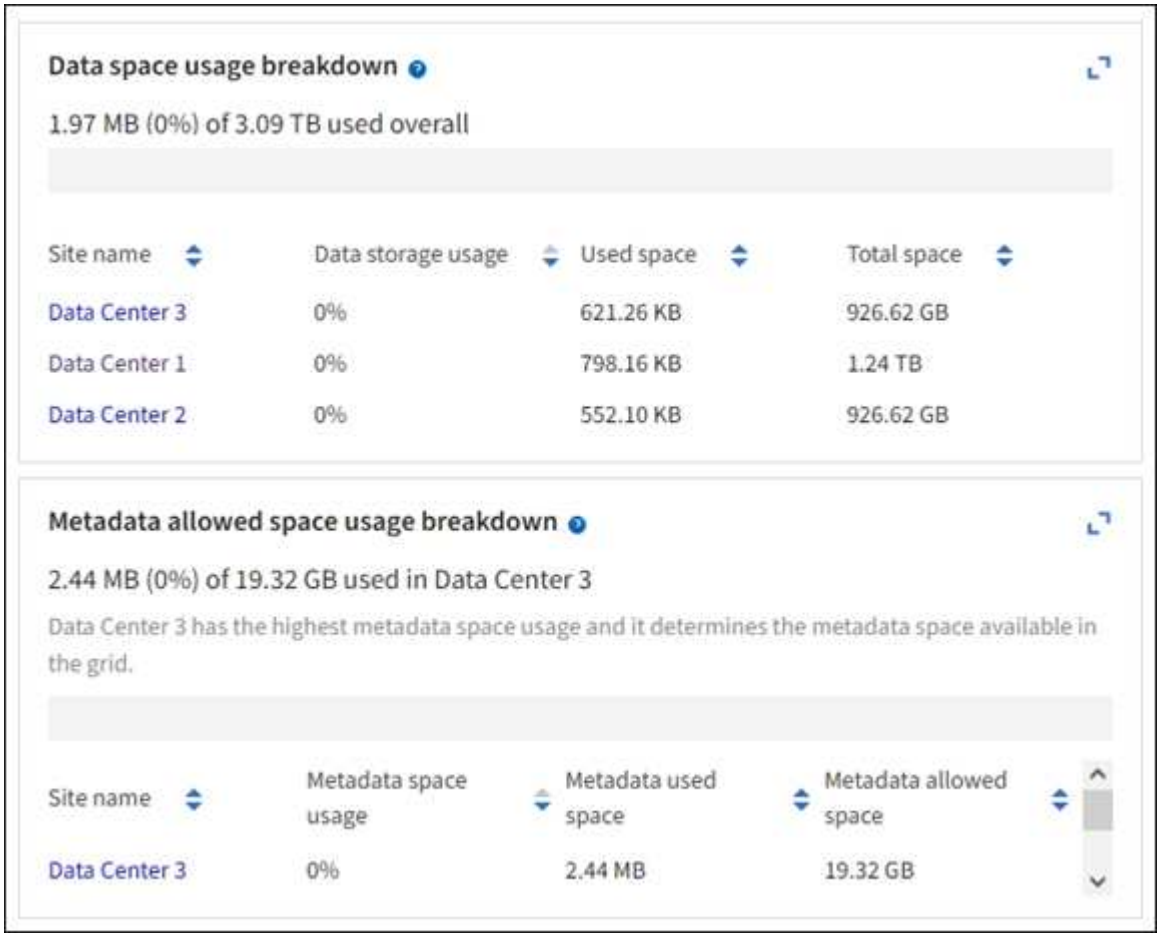
Passos

1. Avalie quanto armazenamento está disponível para toda a grade e para cada data center.

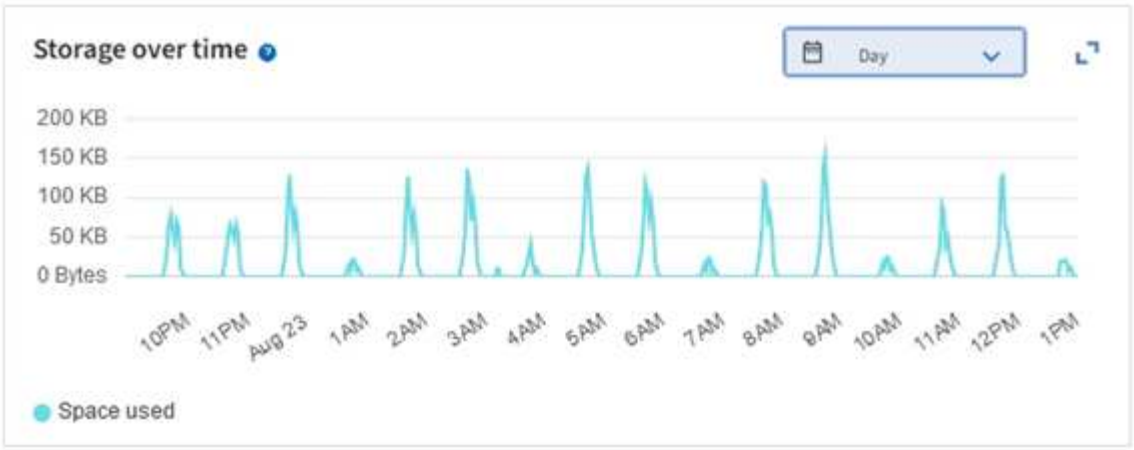
   a. Selecione **Painel > Visão geral**.

   b. Observe os valores nos cartões Detalhamento do uso do espaço de dados e Detalhamento do uso do espaço permitido de metadados. Cada cartão lista uma porcentagem de uso de armazenamento, a capacidade de espaço usado e o espaço total disponível ou permitido pelo site.

      O resumo não inclui mídia de arquivo.



   a. Observe o gráfico no cartão Armazenamento ao longo do tempo. Use o menu suspenso de período de tempo para ajudar a determinar a rapidez com que o armazenamento é consumido.



2. Use a página Nós para obter detalhes adicionais sobre quanto armazenamento foi usado e quanto armazenamento permanece disponível na grade para dados de objetos e metadados de objetos.
   a. Selecione **NODES**.
   b. Selecione ***grid*** > **Armazenamento**.

   c. Posicione o cursor sobre os gráficos **Armazenamento usado - dados do objeto** e **Armazenamento usado - metadados do objeto** para ver quanto armazenamento de objeto e armazenamento de metadados do objeto está disponível para toda a grade e quanto foi usado ao longo do tempo.

> Os valores totais de um site ou da grade não incluem nós que não relataram métricas por pelo menos cinco minutos, como nós offline.

3. Planeje executar uma expansão para adicionar nós de armazenamento ou volumes de armazenamento antes que a capacidade de armazenamento utilizável da grade seja consumida.

   Ao planejar o momento de uma expansão, considere quanto tempo levará para adquirir e instalar armazenamento adicional.

Se sua política de ILM usar codificação de eliminação, talvez você prefira expandir quando os nós de armazenamento existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que devem ser adicionados.

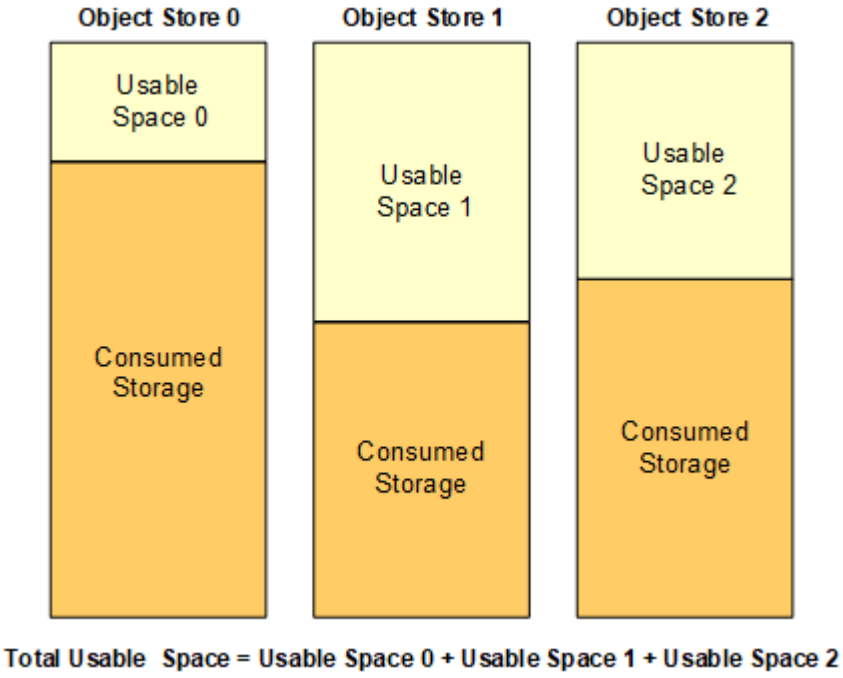
Para obter mais informações sobre o planejamento de uma expansão de armazenamento, consulte o"instruções para expandir o StorageGRID" .

Monitore a capacidade de armazenamento de cada nó de armazenamento

Monitore o espaço total utilizável de cada nó de armazenamento para garantir que o nó tenha espaço suficiente para novos dados de objeto.

Sobre esta tarefa

Espaço utilizável é a quantidade de espaço de armazenamento disponível para armazenar objetos. O espaço total utilizável para um nó de armazenamento é calculado somando o espaço disponível em todos os armazenamentos de objetos dentro do nó.



Passos

1. Selecione **NÓS** > ***Nó de armazenamento*** > **Armazenamento**.

   Os gráficos e tabelas do nó aparecem.

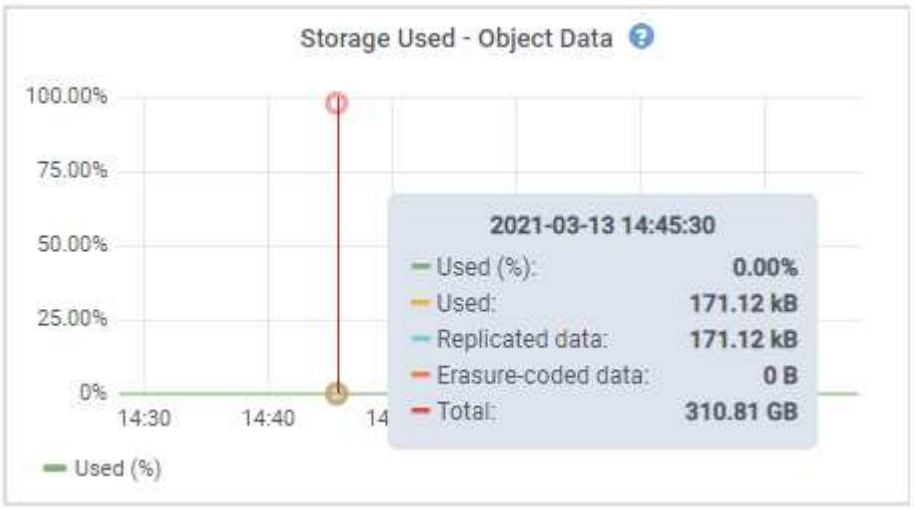
2. Posicione o cursor sobre o gráfico Armazenamento usado - dados do objeto.

   Os seguintes valores são mostrados:

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

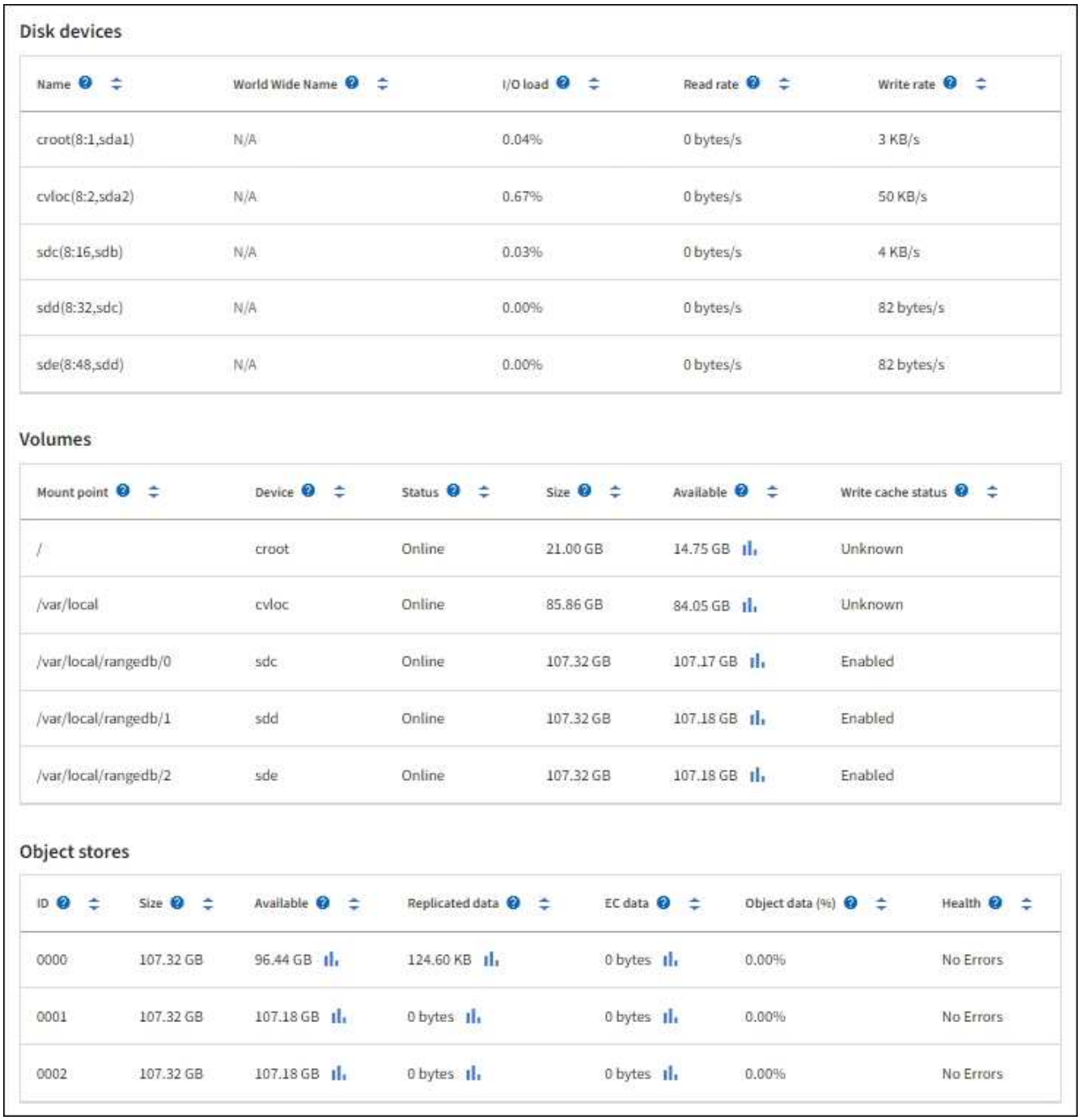
por eliminação neste nó, site ou grade.

- **Total**: A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é o `storagegrid_storage_utilization_data_bytes` métrica.



3. Revise os valores disponíveis nas tabelas Volumes e Armazenamentos de objetos, abaixo dos gráficos.

Para visualizar gráficos desses valores, clique nos ícones do gráfico nas colunas Disponíveis.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Monitore os valores ao longo do tempo para estimar a taxa em que o espaço de armazenamento utilizável está sendo consumido.
5. Para manter as operações normais do sistema, adicione nós de armazenamento, adicione volumes de armazenamento ou arquive dados de objetos antes que o espaço utilizável seja consumido.

   Ao planejar o momento de uma expansão, considere quanto tempo levará para adquirir e instalar armazenamento adicional.

   > Se sua política de ILM usar codificação de eliminação, talvez você prefira expandir quando os nós de armazenamento existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que devem ser adicionados.

   Para obter mais informações sobre o planejamento de uma expansão de armazenamento, consulte

o"instruções para expandir o StorageGRID" .

O"Armazenamento de dados de objetos baixos" O alerta é acionado quando não há espaço suficiente para armazenar dados de objetos em um nó de armazenamento.

Monitorar a capacidade de metadados do objeto para cada nó de armazenamento

Monitore o uso de metadados para cada nó de armazenamento para garantir que haja espaço adequado disponível para operações essenciais do banco de dados. Você deve adicionar novos nós de armazenamento em cada site antes que os metadados do objeto excedam 100% do espaço de metadados permitido.

Sobre esta tarefa

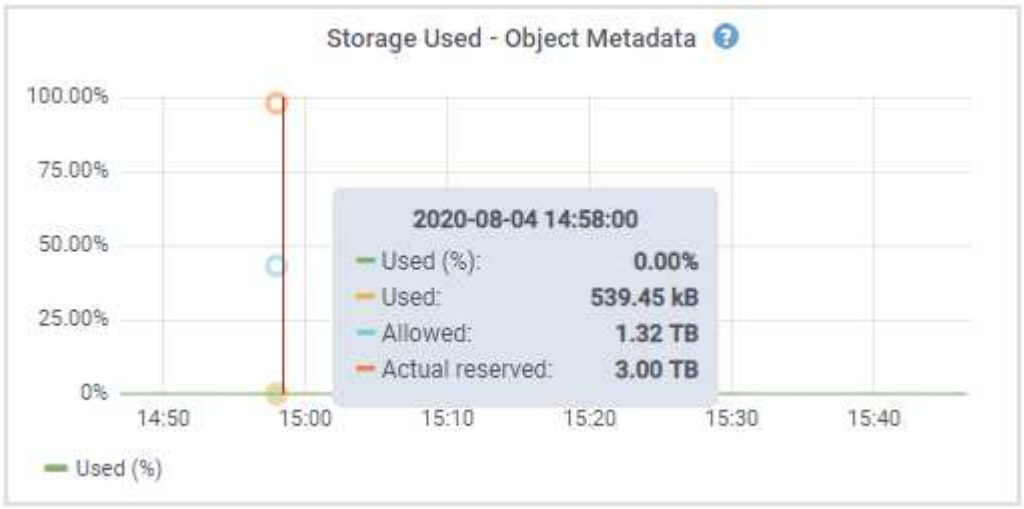
O StorageGRID mantém três cópias de metadados de objetos em cada site para fornecer redundância e proteger os metadados de objetos contra perdas. As três cópias são distribuídas uniformemente entre todos os nós de armazenamento em cada site, usando o espaço reservado para metadados no volume de armazenamento 0 de cada nó de armazenamento.

Em alguns casos, a capacidade de metadados de objetos da grade pode ser consumida mais rapidamente do que sua capacidade de armazenamento de objetos. Por exemplo, se você normalmente ingere grandes quantidades de objetos pequenos, pode ser necessário adicionar nós de armazenamento para aumentar a capacidade de metadados, mesmo que ainda haja capacidade de armazenamento de objetos suficiente.

Alguns dos fatores que podem aumentar o uso de metadados incluem o tamanho e a quantidade de metadados e tags do usuário, o número total de partes em um upload multiparte e a frequência de alterações nos locais de armazenamento do ILM.

Passos

1. Selecione **NÓS** > ***Nó de armazenamento*** > **Armazenamento**.
2. Posicione o cursor sobre o gráfico Armazenamento usado - metadados do objeto para ver os valores de um período específico.



Usado (%)

A porcentagem do espaço de metadados permitido que foi usado neste nó de armazenamento.

Métricas do Prometheus: `storagegrid_storage_utilization_metadata_bytes` e `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

Os bytes do espaço de metadados permitido que foram usados neste nó de armazenamento.

Métrica do Prometeu: `storagegrid_storage_utilization_metadata_bytes`

Permitido

O espaço permitido para metadados de objetos neste nó de armazenamento. Para saber como esse valor é determinado para cada nó de armazenamento, consulte o"descrição completa do espaço de metadados permitido" .

Métrica do Prometeu: `storagegrid_storage_utilization_metadata_allowed_bytes`

Reservado atualmente

O espaço real reservado para metadados neste nó de armazenamento. Inclui o espaço permitido e o espaço necessário para operações essenciais de metadados. Para saber como esse valor é calculado para cada nó de armazenamento, consulte o"descrição completa do espaço reservado real para metadados" .

A métrica Prometheus será adicionada em uma versão futura.

Os valores totais de um site ou da grade não incluem nós que não relataram métricas por pelo menos cinco minutos, como nós offline.

3. Se o valor **Usado (%)** for 70% ou superior, expanda seu sistema StorageGRID adicionando nós de armazenamento a cada site.

O alerta **Baixo armazenamento de metadados** é acionado quando o valor **Usado (%)** atinge determinados limites. Resultados indesejados podem ocorrer se os metadados do objeto usarem mais de 100% do espaço permitido.

Quando você adiciona novos nós, o sistema reequilibra automaticamente os metadados do objeto em todos os nós de armazenamento do site. Veja o"instruções para expandir um sistema StorageGRID" .

Monitorar previsões de uso do espaço

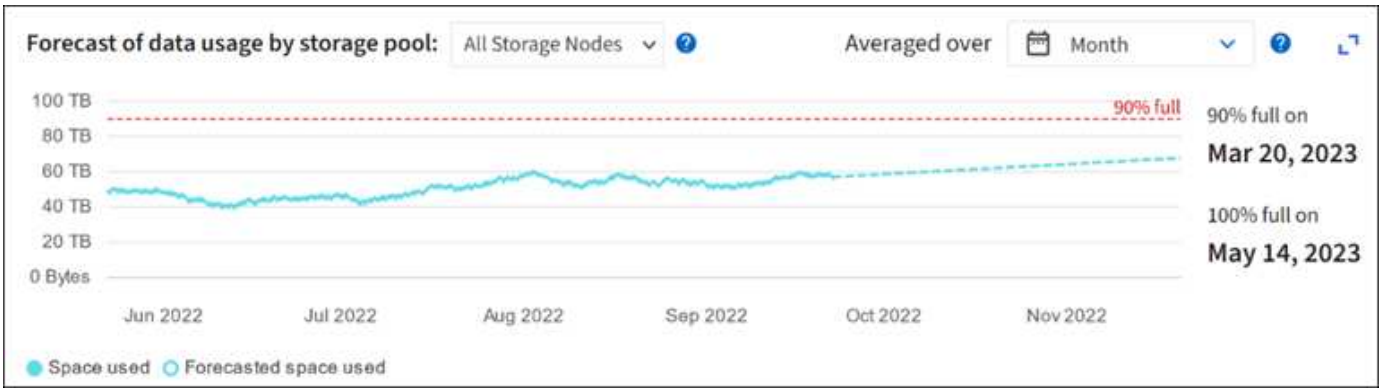
Monitore as previsões de uso do espaço para dados e metadados do usuário para estimar quando você precisará"expandir uma grade" .

Se você notar que a taxa de consumo muda ao longo do tempo, selecione um intervalo menor no menu suspenso **Média sobre** para refletir apenas os padrões de ingestão mais recentes. Se você notar padrões sazonais, selecione um intervalo maior.

Se você tiver uma nova instalação do StorageGRID , permita que dados e metadados se acumulem antes de avaliar as previsões de uso do espaço.

Passos

1. No painel, selecione **Armazenamento**.
2. Visualize os cartões do painel, Previsão de uso de dados por pool de armazenamento e Previsão de uso de metadados por site.
3. Use esses valores para estimar quando você precisará adicionar novos nós de armazenamento para armazenamento de dados e metadados.



Monitorar o gerenciamento do ciclo de vida das informações

O sistema de gerenciamento do ciclo de vida da informação (ILM) fornece gerenciamento de dados para todos os objetos armazenados na grade. Você deve monitorar as operações do ILM para entender se a rede pode lidar com a carga atual ou se mais recursos são necessários.

Sobre esta tarefa

O sistema StorageGRID gerencia objetos aplicando as políticas de ILM ativas. As políticas do ILM e as regras associadas do ILM determinam quantas cópias são feitas, o tipo de cópias que são criadas, onde as cópias são colocadas e por quanto tempo cada cópia é retida.

A ingestão de objetos e outras atividades relacionadas a objetos podem exceder a taxa na qual o StorageGRID pode avaliar o ILM, fazendo com que o sistema enfileire objetos cujas instruções de posicionamento do ILM não podem ser atendidas quase em tempo real. Você deve monitorar se o StorageGRID está acompanhando as ações do cliente.

Use a guia do painel do Grid Manager

Passos

Use a guia ILM no painel do Grid Manager para monitorar as operações do ILM:

1. Sign in no Grid Manager.
2. No painel, selecione a guia ILM e anote os valores no cartão Fila ILM (Objetos) e no cartão Taxa de avaliação ILM.

   Picos temporários no cartão da fila ILM (Objetos) no painel são esperados. Mas se a fila continuar a aumentar e nunca diminuir, a grade precisará de mais recursos para operar com eficiência: mais nós de armazenamento ou, se a política de ILM colocar objetos em locais remotos, mais largura de banda de rede.

Use a página NODES

Passos

Além disso, investigue as filas do ILM usando a página **NODES**:

> Os gráficos na página **NODES** serão substituídos pelos cartões do painel correspondentes em uma versão futura do StorageGRID .

1. Selecione **NODES**.
2. Selecione ***nome da grade*** > **ILM**.
3. Posicione o cursor sobre o gráfico de fila do ILM para ver o valor dos seguintes atributos em um determinado momento:
   - **Objetos na fila (de operações do cliente)**: O número total de objetos aguardando avaliação do ILM devido a operações do cliente (por exemplo, ingestão).
   - **Objetos na fila (de todas as operações)**: O número total de objetos aguardando avaliação do ILM.
   - **Taxa de varredura (objetos/seg)**: A taxa na qual os objetos na grade são varridos e colocados na fila para ILM.
   - **Taxa de avaliação (objetos/seg)**: A taxa atual na qual os objetos estão sendo avaliados em relação à política de ILM na grade.
4. Na seção Fila do ILM, observe os seguintes atributos.

   A seção da fila ILM está incluída somente para a grade. Essas informações não são mostradas na guia ILM de um site ou nó de armazenamento.

   - **Período de verificação - estimado**: Tempo estimado para concluir uma verificação ILM completa de todos os objetos.

     Uma verificação completa não garante que o ILM foi aplicado a todos os objetos.

   - **Reparos tentados**: O número total de operações de reparo de objetos para dados replicados que foram tentadas. Essa contagem aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Reparos de ILM de alto risco são priorizados se a rede ficar ocupada.

     O mesmo reparo de objeto pode ser incrementado novamente se a replicação falhar após o reparo.

   Esses atributos podem ser úteis ao monitorar o progresso da recuperação do volume do nó de armazenamento. Se o número de reparos tentados parou de aumentar e uma verificação completa foi concluída, o reparo provavelmente foi concluído.

Monitorar recursos de rede e sistema

A integridade e a largura de banda da rede entre nós e sites, bem como o uso de recursos por nós de grade individuais, são essenciais para operações eficientes.

Monitore as conexões e o desempenho da rede

A conectividade de rede e a largura de banda são especialmente importantes se sua política de gerenciamento do ciclo de vida das informações (ILM) copiar objetos replicados entre sites ou armazenar objetos codificados para eliminação usando um esquema que forneça proteção contra perda de site. Se a rede entre os sites não estiver disponível, a latência da rede for muito alta ou a largura de banda da rede for insuficiente, algumas regras de ILM podem não conseguir colocar objetos onde esperado. Isso pode levar a falhas de ingestão (quando a opção Ingestão estrita é selecionada para regras de ILM) ou a baixo desempenho de ingestão e pendências de ILM.

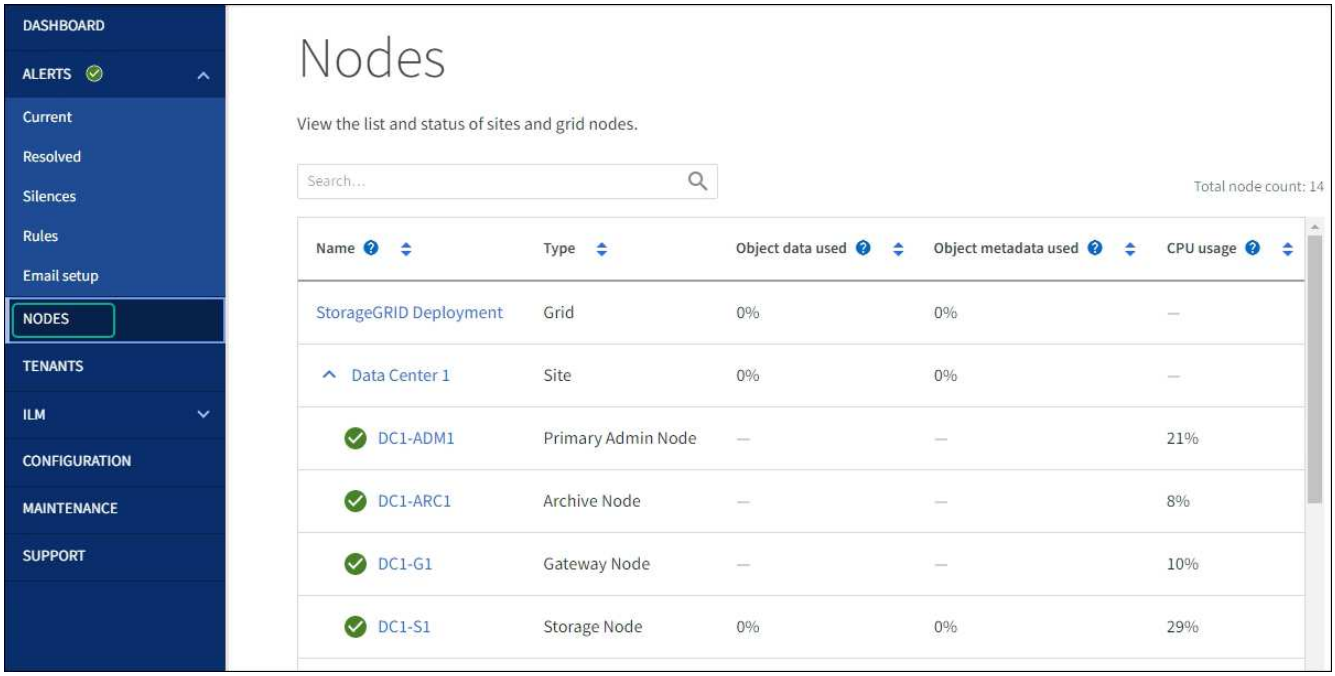
Use o Grid Manager para monitorar a conectividade e o desempenho da rede para que você possa resolver quaisquer problemas imediatamente.

Além disso, considere"criando políticas de classificação de tráfego de rede" para que você possa monitorar o tráfego relacionado a locatários, buckets, sub-redes ou endpoints de balanceador de carga específicos. Você pode definir políticas de limitação de tráfego conforme necessário.

Passos

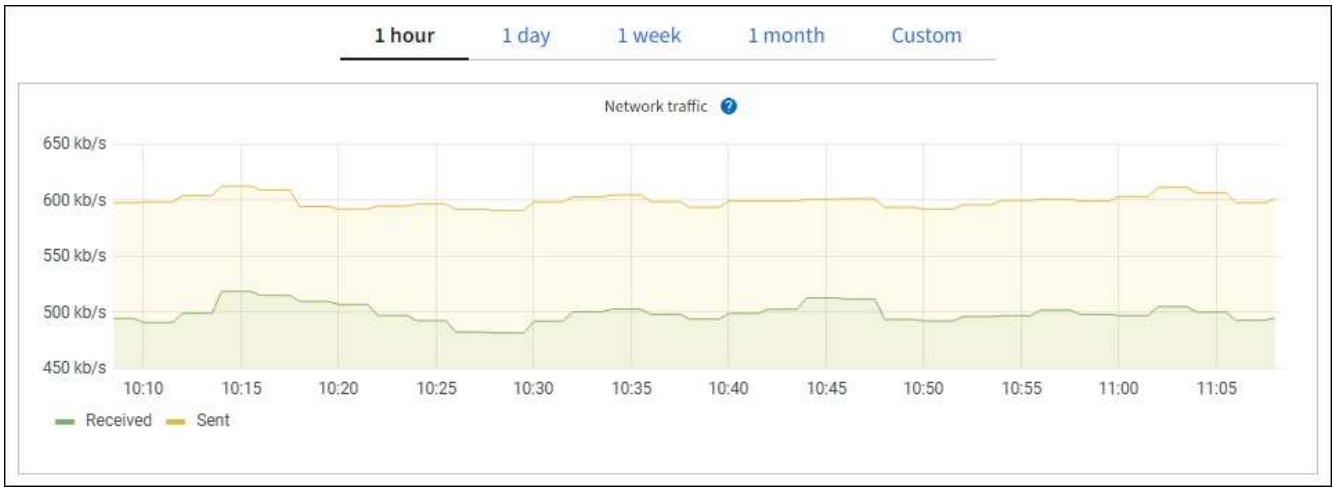
1. Selecione **NODES**.

   A página Nós é exibida. Cada nó na grade é listado em formato de tabela.

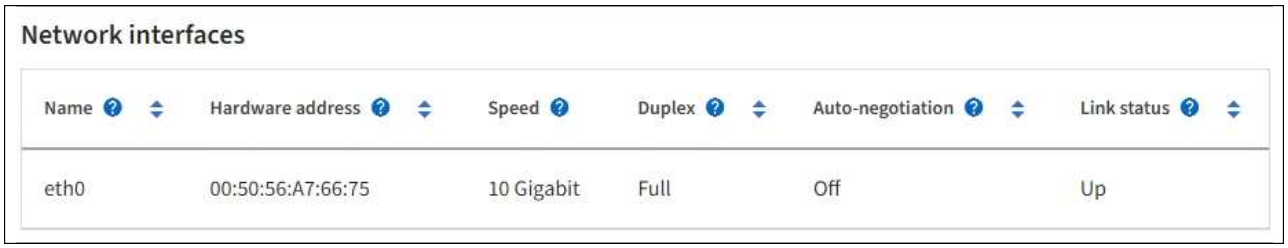


2. Selecione o nome da grade, um site de data center específico ou um nó da grade e, em seguida, selecione a guia **Rede**.

   O gráfico de tráfego de rede fornece um resumo do tráfego geral de rede para a grade como um todo, para o site do data center ou para o nó.

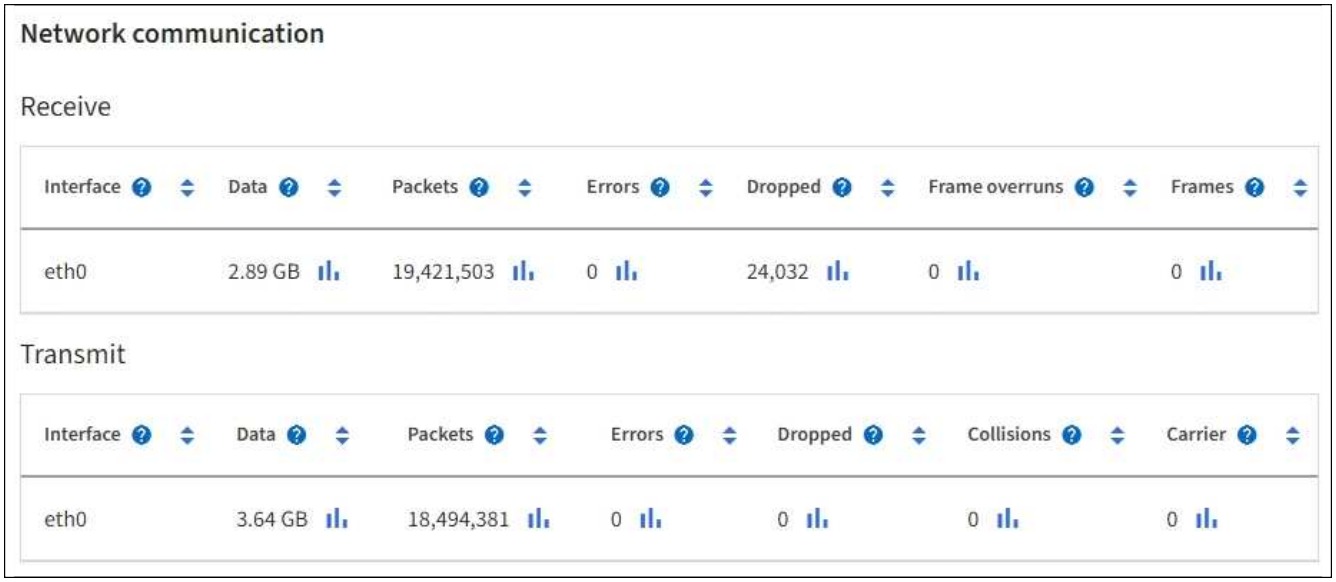


   a. Se você selecionou um nó de grade, role para baixo para revisar a seção **Interfaces de rede** da página.



b. Para nós de grade, role para baixo para revisar a seção **Comunicação de rede** da página.

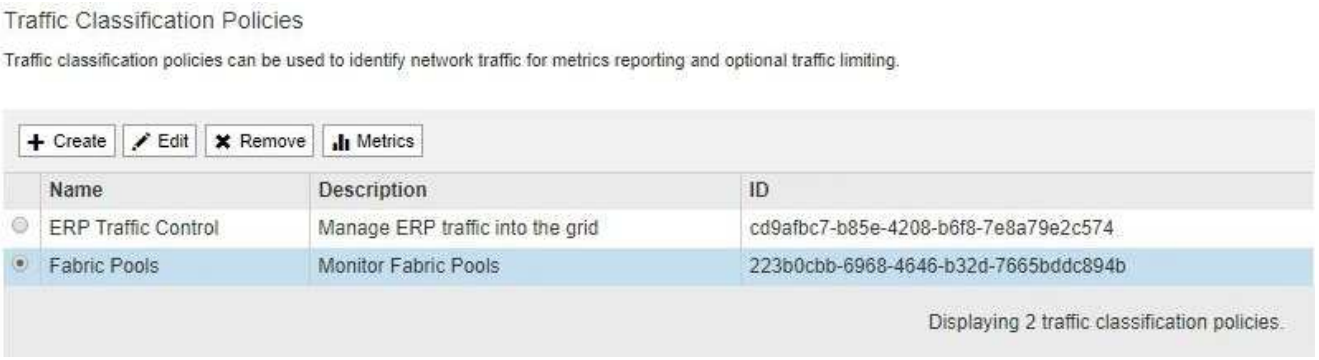
   As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.



3. Use as métricas associadas às suas políticas de classificação de tráfego para monitorar o tráfego de rede.

   a. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.

      A página Políticas de Classificação de Tráfego é exibida e as políticas existentes são listadas na tabela.



   a. Para visualizar gráficos que mostram as métricas de rede associadas a uma política, selecione o botão de opção à esquerda da política e clique em **Métricas**.

   b. Revise os gráficos para entender o tráfego de rede associado à política.

      Se uma política de classificação de tráfego for projetada para limitar o tráfego de rede, analise com que frequência o tráfego é limitado e decida se a política continua atendendo às suas necessidades.

De tempos em tempos,"ajuste cada política de classificação de tráfego conforme necessário" .

Informações relacionadas

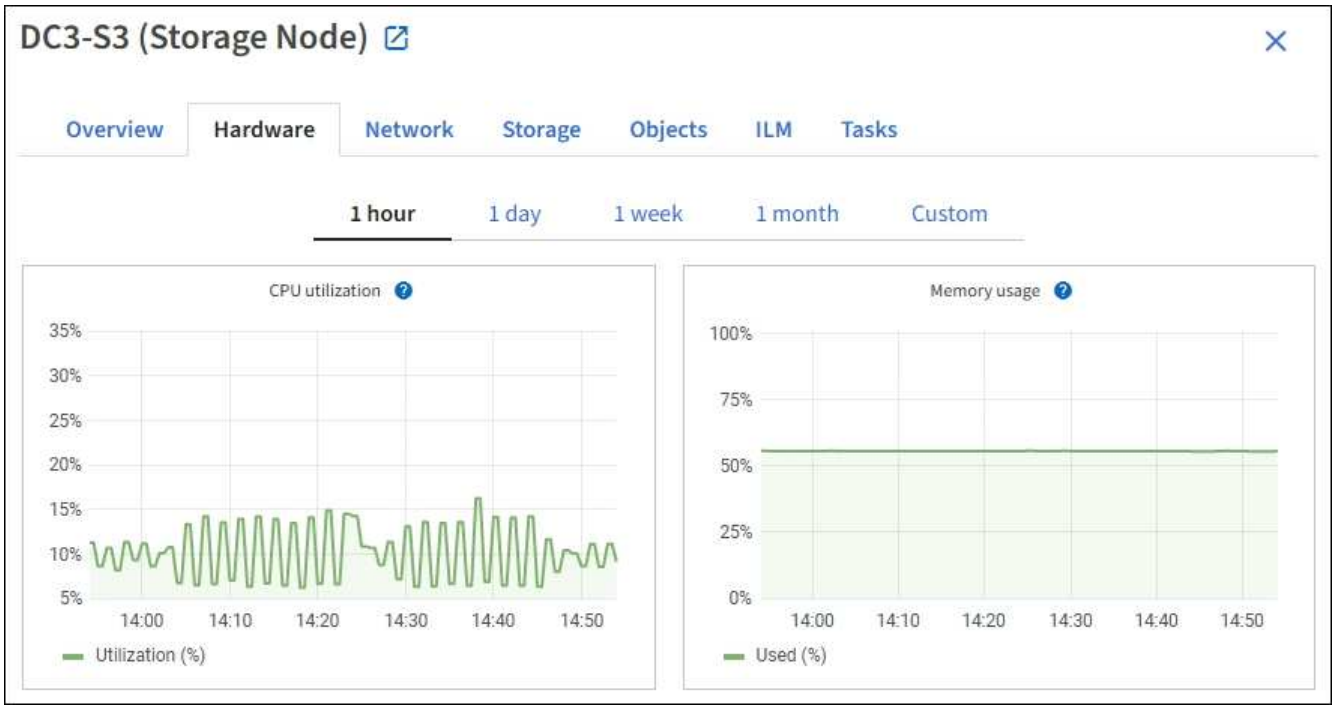
- "Ver a aba Rede"
- "Monitorar estados de conexão de nós"

Monitorar recursos em nível de nó

Monitore nós de grade individuais para verificar seus níveis de uso de recursos. Se os nós estiverem constantemente sobrecarregados, mais nós poderão ser necessários para operações eficientes.

Passos

1. Na página **NÓS**, selecione o nó.
2. Selecione a aba **Hardware** para exibir gráficos de Utilização da CPU e Uso da Memória.



3. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.
4. Se o nó estiver hospedado em um dispositivo de armazenamento ou de serviços, role para baixo para visualizar as tabelas de componentes. O status de todos os componentes deve ser "Nominal". Investigue componentes que tenham qualquer outro status.

Informações relacionadas

- "Exibir informações sobre nós de armazenamento do dispositivo"
- "Exibir informações sobre nós de administração e nós de gateway do dispositivo"

Monitorar a atividade do inquilino

Todas as atividades do cliente S3 estão associadas às contas de locatário do StorageGRID . Você pode usar o Grid Manager para monitorar o uso de armazenamento

ou o tráfego de rede para todos os locatários ou um locatário específico. Você pode usar o log de auditoria ou os painéis do Grafana para coletar informações mais detalhadas sobre como os locatários estão usando o StorageGRID.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou contas de locatário" .

Ver todos os inquilinos

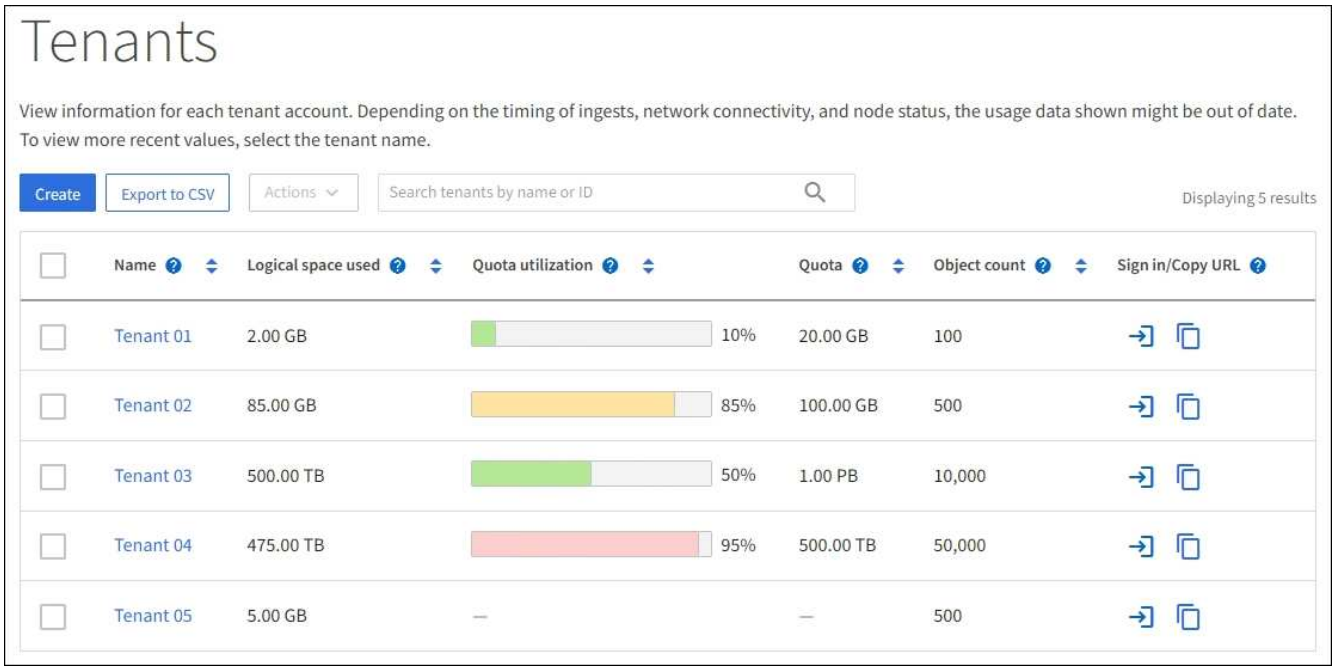
A página Inquilinos mostra informações básicas para todas as contas de inquilinos atuais.

Passos

1. Selecione **LOCATÁRIOS**.
2. Revise as informações mostradas nas páginas do Locatário.

   O espaço lógico usado, o uso da cota, a cota e a contagem de objetos são listados para cada locatário. Se uma cota não for definida para um locatário, os campos Uso de cota e Cota conterão um hífen (—).

   > Os valores de espaço utilizado são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó.



3. Opcionalmente, faça login em uma conta de locatário selecionando o link de login na coluna * Sign in/Copiar URL*.
4. Opcionalmente, copie o URL da página de login de um locatário selecionando o link copiar URL na coluna * Sign in/Copiar URL*.
5. Opcionalmente, selecione **Exportar para CSV** para visualizar e exportar um `.csv` arquivo contendo os valores de uso para todos os locatários.

   Você será solicitado a abrir ou salvar o `.csv` arquivo.

O conteúdo do `.csv` arquivo se parece com o exemplo a seguir:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

Você pode abrir o `.csv` arquivar em um aplicativo de planilha ou usá-lo em automação.

6. Se nenhum objeto estiver listado, opcionalmente, selecione **Ações** > **Excluir** para remover um ou mais inquilinos. Ver "Excluir conta de inquilino" .

   Não é possível remover uma conta de locatário se ela incluir buckets ou contêineres.

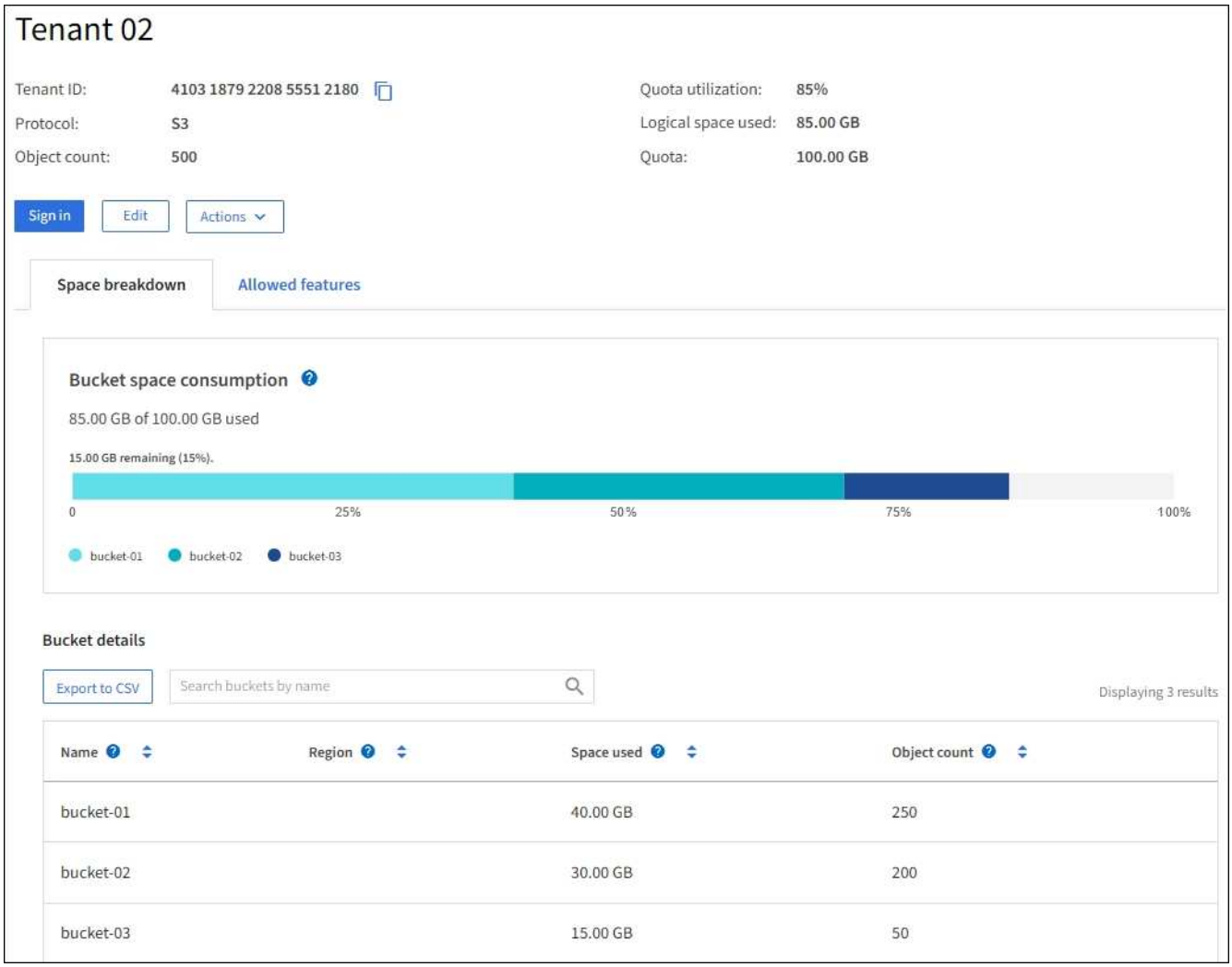
Ver um inquilino específico

Você pode visualizar detalhes de um inquilino específico.

Passos

1. Selecione o nome do inquilino na página Inquilinos.

   A página de detalhes do inquilino é exibida.



2. Revise a visão geral do inquilino no topo da página.

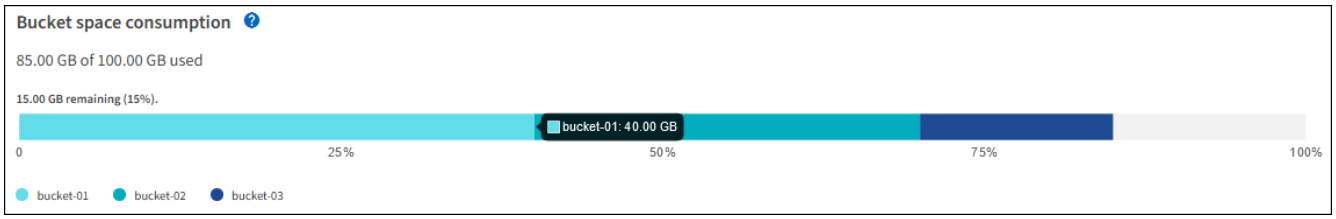
   Esta seção da página de detalhes fornece informações resumidas sobre o locatário, incluindo a contagem de objetos do locatário, o uso da cota, o espaço lógico usado e a configuração da cota.

3. Na aba **Detalhamento de espaço**, revise o gráfico **Consumo de espaço**.

   Este gráfico mostra o consumo total de espaço para todos os buckets S3 do locatário.

   Se uma cota foi definida para este locatário, a quantidade de cota usada e restante será exibida em texto (por exemplo, `85.00 GB of 100 GB used`). Se nenhuma cota foi definida, o locatário tem uma cota ilimitada e o texto inclui apenas uma quantidade de espaço usado (por exemplo, `85.00 GB used`). O gráfico de barras mostra a porcentagem de cota em cada balde ou contêiner. Se o locatário tiver excedido a cota de armazenamento em mais de 1% e em pelo menos 1 GB, o gráfico mostrará a cota total e o valor excedente.

   Você pode colocar o cursor sobre o gráfico de barras para ver o armazenamento usado por cada bucket ou contêiner. Você pode colocar o cursor sobre o segmento de espaço livre para ver a quantidade de cota de armazenamento restante.



O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novas ingestões se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em consideração o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que o uso da cota seja recalculado. Os cálculos de uso de cota podem levar 10 minutos ou mais.

O uso de cota de um locatário indica a quantidade total de dados de objeto que o locatário carregou no StorageGRID (tamanho lógico). O uso da cota não representa o espaço usado para armazenar cópias desses objetos e seus metadados (tamanho físico).

Você pode habilitar a regra de alerta **Uso alto de cota de locatário** para determinar se os locatários estão consumindo suas cotas. Se habilitado, esse alerta será acionado quando um locatário tiver usado 90% de sua cota. Para obter instruções, consulte"Editar regras de alerta" .

4. Na aba **Detalhamento do espaço**, revise os **Detalhes do bucket**.

   Esta tabela lista os buckets do S3 para o locatário. O espaço usado é a quantidade total de dados de objeto no bucket ou contêiner. Este valor não representa o espaço de armazenamento necessário para cópias do ILM e metadados de objetos.

5. Opcionalmente, selecione **Exportar para CSV** para visualizar e exportar um arquivo .csv contendo os valores de uso para cada bucket ou contêiner.

   O conteúdo de um locatário S3 individual `.csv` arquivo se parece com o exemplo a seguir:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   Você pode abrir o `.csv` arquivar em um aplicativo de planilha ou usá-lo em automação.

6. Opcionalmente, selecione a aba **Recursos permitidos** para ver uma lista de permissões e recursos habilitados para o locatário. Ver"Editar conta de inquilino" se você precisar alterar qualquer uma dessas configurações.
7. Se o locatário tiver a permissão **Usar conexão de federação de grade**, selecione opcionalmente a guia **Federação de grade** para saber mais sobre a conexão.

   Ver"O que é federação de grade?" e"Gerenciar os inquilinos permitidos para federação de rede" .

Exibir tráfego de rede

Se houver políticas de classificação de tráfego em vigor para um locatário, revise o tráfego de rede desse locatário.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.

   A página Políticas de Classificação de Tráfego é exibida e as políticas existentes são listadas na tabela.

2. Revise a lista de políticas para identificar aquelas que se aplicam a um inquilino específico.
3. Para visualizar métricas associadas a uma política, selecione o botão de opção à esquerda da política e selecione **Métricas**.
4. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustá-la.

Ver "Gerenciar políticas de classificação de tráfego" para maiores informações.

Use o log de auditoria

Opcionalmente, você pode usar o log de auditoria para um monitoramento mais granular das atividades de um locatário.

Por exemplo, você pode monitorar os seguintes tipos de informações:

- Operações específicas do cliente, como PUT, GET ou DELETE
- Tamanhos de objetos
- A regra ILM aplicada a objetos
- O IP de origem das solicitações do cliente

Os logs de auditoria são gravados em arquivos de texto que você pode analisar usando a ferramenta de análise de logs de sua escolha. Isso permite que você entenda melhor as atividades do cliente ou implemente modelos sofisticados de cobrança e estorno.

Ver "Revisar logs de auditoria" para maiores informações.

Use métricas do Prometheus

Opcionalmente, use as métricas do Prometheus para relatar a atividade do locatário.

- No Grid Manager, selecione **SUPORTE** > **Ferramentas** > **Métricas**. Você pode usar painéis existentes, como o S3 Overview, para revisar as atividades do cliente.

  > As ferramentas disponíveis na página Métricas destinam-se principalmente ao uso do suporte técnico. Alguns recursos e itens de menu nessas ferramentas são intencionalmente não funcionais.

- Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**. Você pode usar as métricas na seção Métricas da API de gerenciamento de grade para criar regras de alerta e painéis personalizados para a atividade do locatário.

Ver "Revisar métricas de suporte" para maiores informações.

Monitorar operações do cliente S3

Você pode monitorar as taxas de ingestão e recuperação de objetos, bem como métricas para contagens, consultas e verificação de objetos. Você pode visualizar o número de tentativas bem-sucedidas e malsucedidas de aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID .

Antes de começar

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

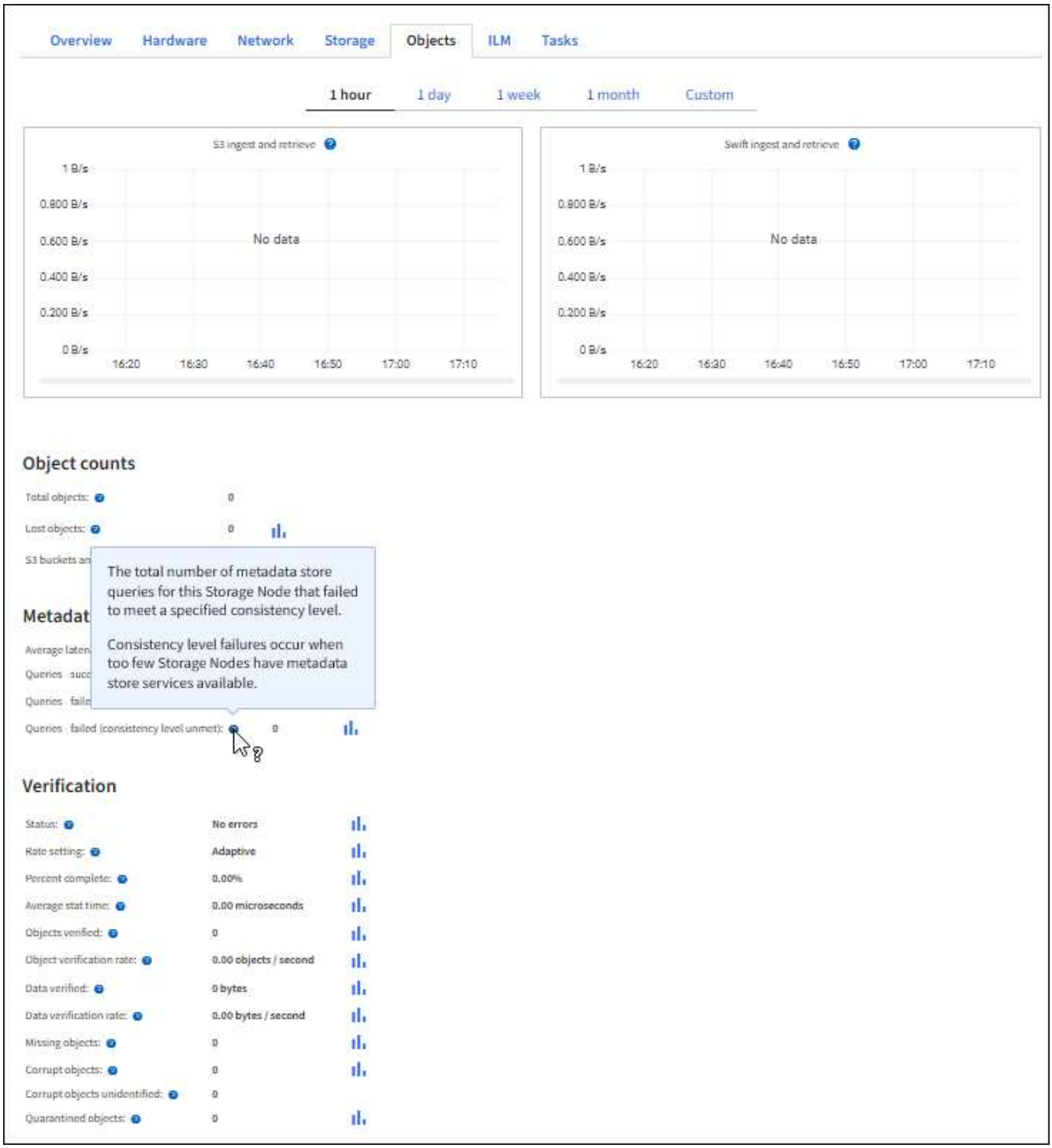
Passos

1. No painel, selecione a aba **Desempenho**.
2. Consulte os gráficos do S3, que resumem o número de operações de cliente executadas pelos nós de armazenamento e o número de solicitações de API recebidas pelos nós de armazenamento durante o período selecionado.
3. Selecione **NÓS** para acessar a página Nós.
4. Na página inicial dos Nós (nível de grade), selecione a aba **Objetos**.

   O gráfico mostra as taxas de ingestão e recuperação do S3 para todo o seu sistema StorageGRID em bytes por segundo e a quantidade de dados ingeridos ou recuperados. Você pode selecionar um intervalo de tempo ou aplicar um intervalo personalizado.

5. Para ver informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e selecione a guia **Objetos**.

   O gráfico mostra as taxas de ingestão e recuperação do nó. A guia também inclui métricas para contagens de objetos, consultas de metadados e operações de verificação.



Monitorar operações de balanceamento de carga

Se estiver usando um balanceador de carga para gerenciar conexões de clientes com o StorageGRID, você deverá monitorar as operações de balanceamento de carga depois de configurar o sistema inicialmente e depois de fazer qualquer alteração de configuração ou executar uma expansão.

Sobre esta tarefa

Você pode usar o serviço Load Balancer em nós de administração ou nós de gateway ou um balanceador de carga externo de terceiros para distribuir solicitações de clientes entre vários nós de armazenamento.

Após configurar o balanceamento de carga, você deve confirmar se as operações de ingestão e recuperação de objetos estão sendo distribuídas uniformemente entre os nós de armazenamento. Solicitações distribuídas uniformemente garantem que o StorageGRID permaneça responsivo às solicitações do cliente sob carga e podem ajudar a manter o desempenho do cliente.

Se você configurou um grupo de alta disponibilidade (HA) de nós de gateway ou nós de administração no modo de backup ativo, somente um nó no grupo distribui ativamente as solicitações do cliente.

Para obter mais informações, consulte "Configurar conexões do cliente S3" .

Passos

1. Se os clientes S3 se conectarem usando o serviço Load Balancer, verifique se os nós de administração ou os nós de gateway estão distribuindo ativamente o tráfego conforme o esperado:
   a. Selecione **NODES**.
   b. Selecione um nó de gateway ou um nó de administração.
   c. Na guia **Visão geral**, verifique se uma interface de nó está em um grupo de HA e se a interface de nó tem a função de Primária.

      Nós com a função Primário e nós que não estão em um grupo HA devem distribuir ativamente solicitações aos clientes.

   d. Para cada nó que deve distribuir ativamente solicitações de clientes, selecione o"Guia Balanceador de Carga" .
   e. Revise o gráfico de tráfego de solicitações do balanceador de carga da última semana para garantir que o nó esteja distribuindo solicitações ativamente.

      Os nós em um grupo de HA de backup ativo podem assumir a função de Backup de tempos em tempos. Durante esse tempo, os nós não distribuem solicitações de clientes.

   f. Revise o gráfico da Taxa de Solicitações de Entrada do Balanceador de Carga da última semana para analisar a taxa de transferência de objetos do nó.
   g. Repita essas etapas para cada nó de administração ou nó de gateway no sistema StorageGRID .
   h. Opcionalmente, use políticas de classificação de tráfego para visualizar uma análise mais detalhada do tráfego atendido pelo serviço Load Balancer.
2. Verifique se essas solicitações estão sendo distribuídas uniformemente aos nós de armazenamento.
   a. Selecione ***Nó de armazenamento*** > **LDR** > **HTTP**.
   b. Revise o número de **Sessões de entrada atualmente estabelecidas**.
   c. Repita para cada nó de armazenamento na grade.

      O número de sessões deve ser aproximadamente igual em todos os nós de armazenamento.

Monitorar conexões de federação de rede

Você pode monitorar informações básicas sobre todos"conexões de federação de rede" , informações detalhadas sobre uma conexão específica ou métricas do Prometheus sobre operações de replicação entre redes. Você pode monitorar uma conexão de qualquer uma das redes.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grades usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" para a grade na qual você está conectado.

Ver todas as conexões

A página Federação de grade mostra informações básicas sobre todas as conexões de federação de grade e sobre todas as contas de locatário que têm permissão para usar conexões de federação de grade.

Passos

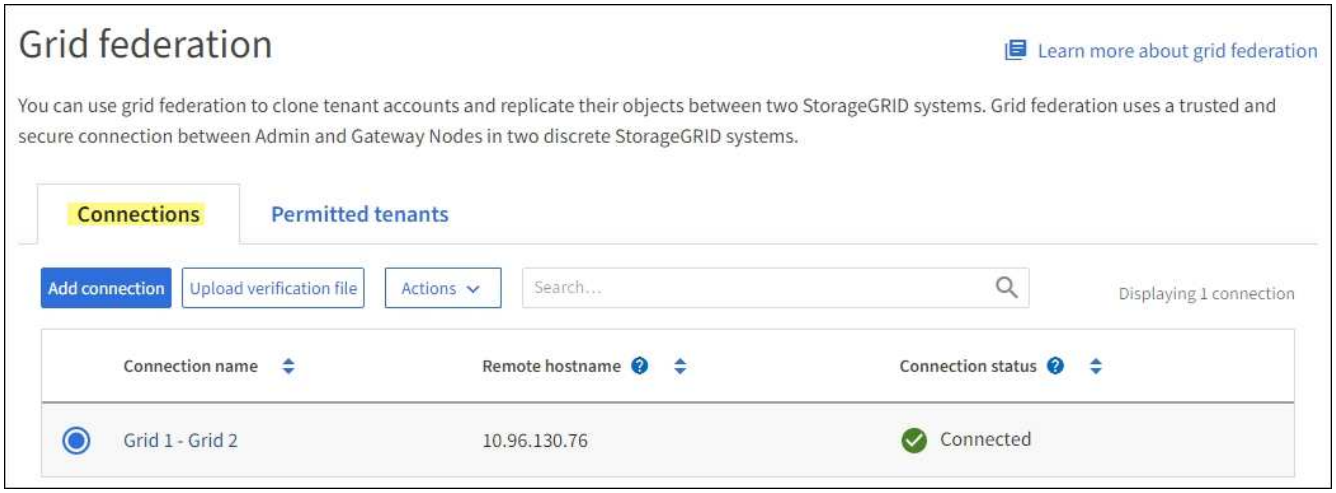
1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.

   A página da federação Grid é exibida.

2. Para ver informações básicas de todas as conexões nesta grade, selecione a aba **Conexões**.

   Nesta aba, você pode:

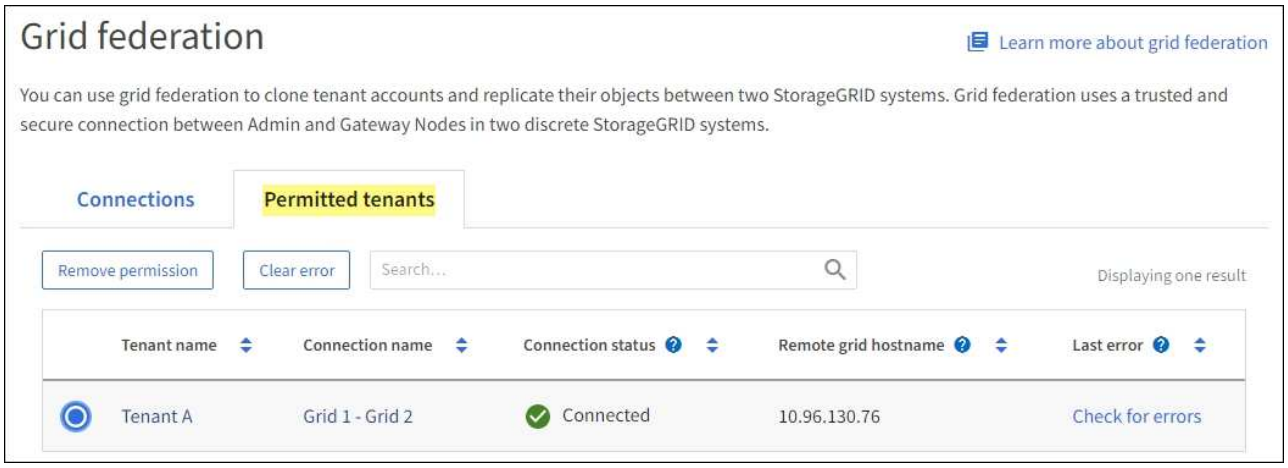
   - "Criar uma nova conexão" .
   - Selecione uma conexão existente para"editar ou testar" .



3. Para ver informações básicas de todas as contas de locatários nesta grade que têm a permissão **Usar conexão de federação de grade**, selecione a guia **Locatários permitidos**.

   Nesta aba, você pode:

   - "Veja a página de detalhes de cada inquilino permitido" .
   - Veja a página de detalhes de cada conexão. Ver Ver uma conexão específica .
   - Selecione um inquilino permitido e"remover a permissão" .
   - Verifique se há erros de replicação entre grades e limpe o último erro, se houver. Ver "Solucionar erros de federação de grade" .



Ver uma conexão específica

Você pode visualizar detalhes de uma conexão de federação de grade específica.

Passos

1. Selecione qualquer uma das guias na página Federação da grade e, em seguida, selecione o nome da conexão na tabela.

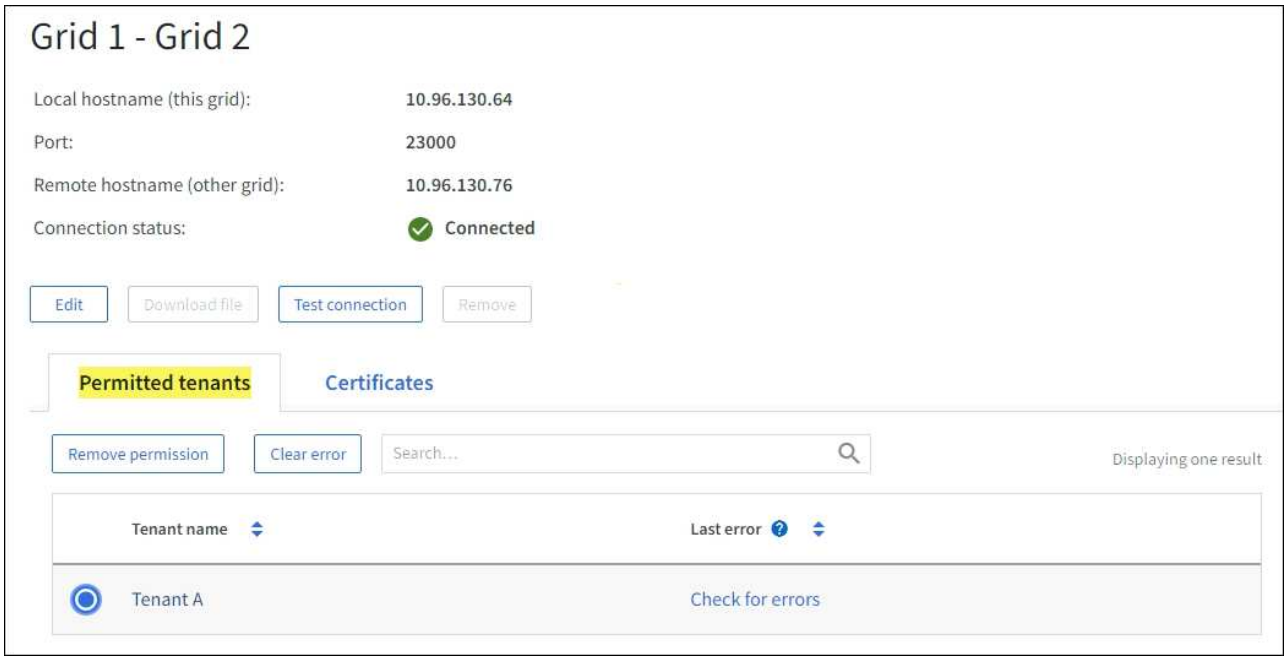
   Na página de detalhes da conexão, você pode:

   - Veja informações básicas de status sobre a conexão, incluindo nomes de host locais e remotos, porta e status da conexão.
   - Selecione uma conexão para"editar, testar ou remover" .

2. Ao visualizar uma conexão específica, selecione a aba **Inquilinos permitidos** para ver detalhes sobre os inquilinos permitidos para a conexão.

   Nesta aba, você pode:

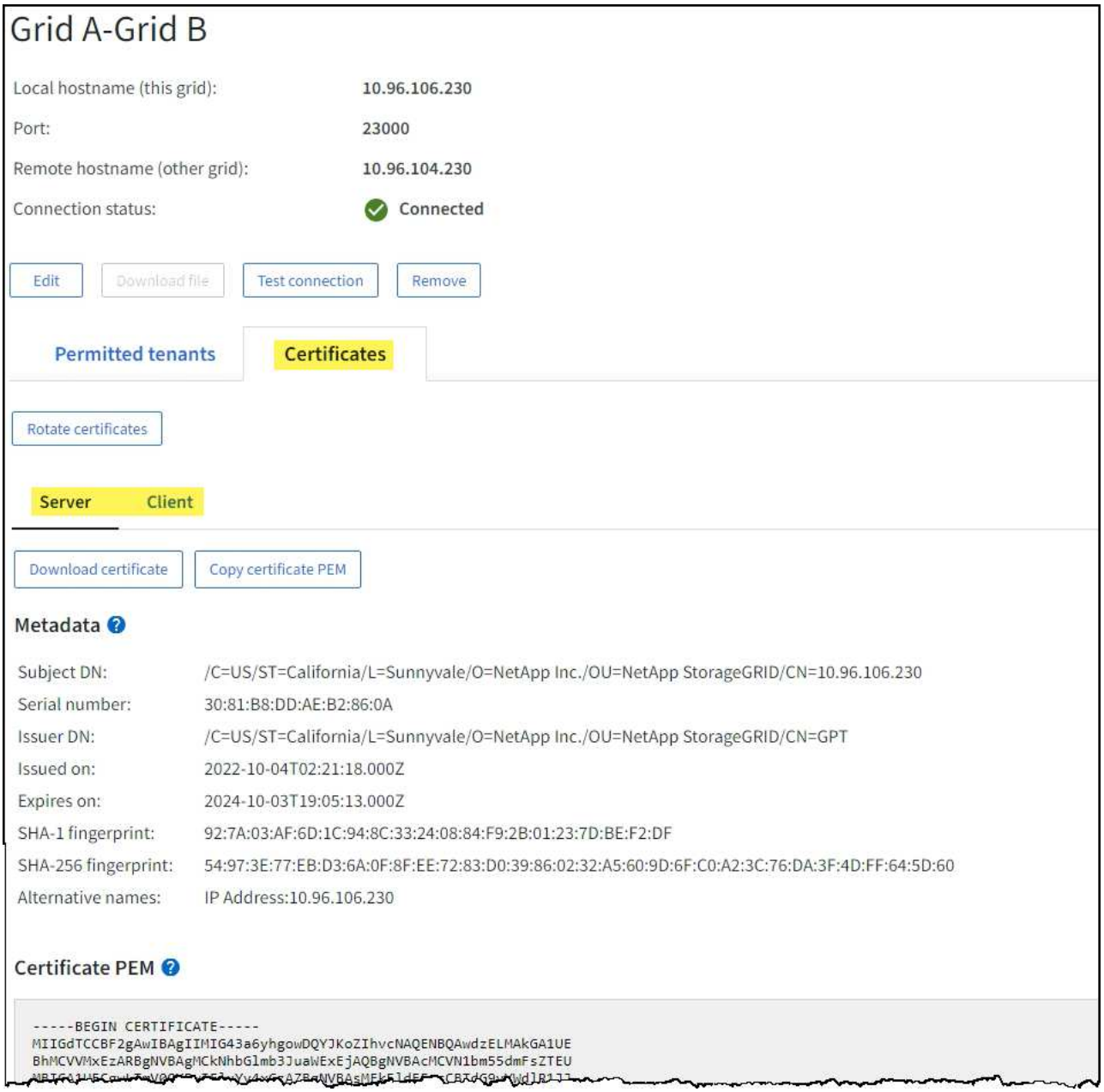
   - "Veja a página de detalhes de cada inquilino permitido" .
   - "Remover a permissão de um inquilino"para usar a conexão.
   - Verifique se há erros de replicação entre grades e limpe o último erro. Ver "Solucionar erros de federação de grade" .



3. Ao visualizar uma conexão específica, selecione a guia **Certificados** para visualizar os certificados de servidor e cliente gerados pelo sistema para esta conexão.

   Nesta aba, você pode:

   - "Girar certificados de conexão" .
   - Selecione **Servidor** ou **Cliente** para visualizar ou baixar o certificado associado ou copiar o certificado PEM.



Revisar métricas de replicação entre grades

Você pode usar o painel de replicação entre grades no Grafana para visualizar métricas do Prometheus sobre operações de replicação entre grades na sua grade.

Passos

1. No Grid Manager, selecione **SUPORTE** > **Ferramentas** > **Métricas**.

> As ferramentas disponíveis na página Métricas são destinadas ao uso do suporte técnico. Alguns recursos e itens de menu dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Veja a lista de"métricas Prometheus comumente usadas" .

2. Na seção Grafana da página, selecione **Cross Grid Replication**.

   Para obter instruções detalhadas, consulte"Revisar métricas de suporte" .

3. Para tentar replicar novamente objetos que falharam na replicação, consulte"Identificar e tentar novamente operações de replicação com falha" .

Gerenciar alertas

Gerenciar alertas

O sistema de alerta fornece uma interface fácil de usar para detectar, avaliar e resolver problemas que podem ocorrer durante a operação do StorageGRID .

Os alertas são acionados em níveis de gravidade específicos quando as condições da regra de alerta são avaliadas como verdadeiras. Quando um alerta é disparado, as seguintes ações ocorrem:

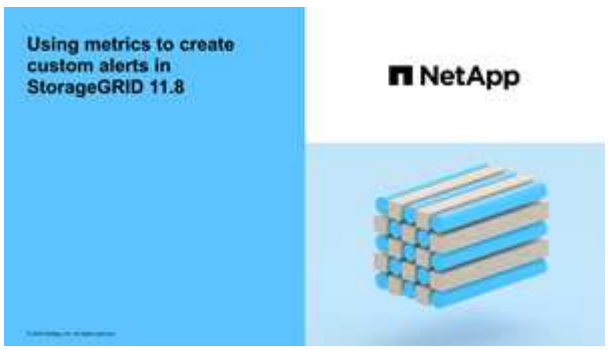
- Um ícone de gravidade de alerta é exibido no painel do Grid Manager, e a contagem de Alertas Atuais é incrementada.
- O alerta é exibido na página de resumo **NODES** e na guia **NODES** > ***node*** > **Overview**.
- Uma notificação por e-mail é enviada, supondo que você tenha configurado um servidor SMTP e fornecido endereços de e-mail para os destinatários.
- Uma notificação do Protocolo Simples de Gerenciamento de Rede (SNMP) é enviada, supondo que você tenha configurado o agente SNMP do StorageGRID .

Você pode criar alertas personalizados, editar ou desabilitar alertas e gerenciar notificações de alertas.

Para saber mais:

- Reveja o vídeo: "Vídeo: Visão geral dos alertas"

- Reveja o vídeo: "Vídeo: Alertas personalizados"



- Veja o"Referência de alertas" .

Ver regras de alerta

As regras de alerta definem as condições que desencadeiam"alertas específicos" . O StorageGRID inclui um conjunto de regras de alerta padrão, que você pode usar como estão ou modificar, ou pode criar regras de alerta personalizadas.

Você pode visualizar a lista de todas as regras de alerta padrão e personalizadas para saber quais condições acionarão cada alerta e para ver se algum alerta está desabilitado.

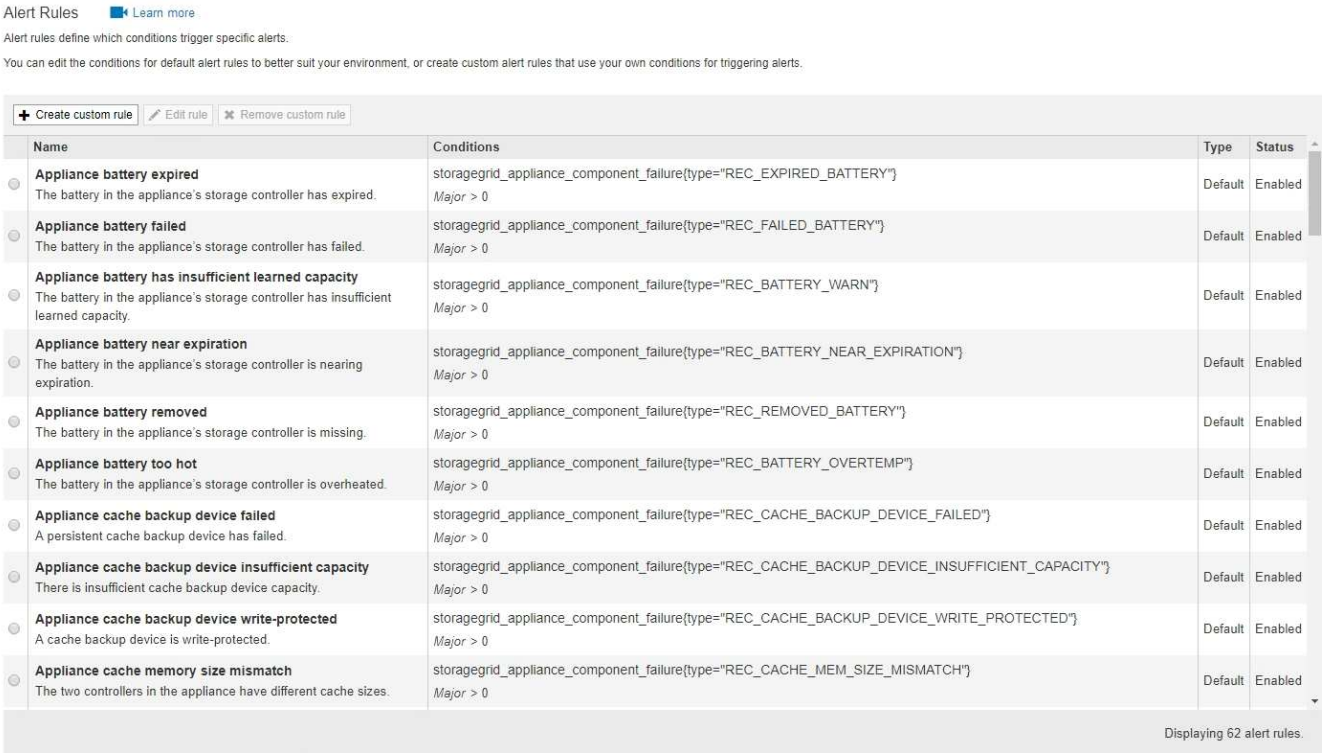
Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .
- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral dos alertas"

Passos

1. Selecione **ALERTAS** > **Regras**.

   A página Regras de alerta é exibida.



2. Revise as informações na tabela de regras de alerta:

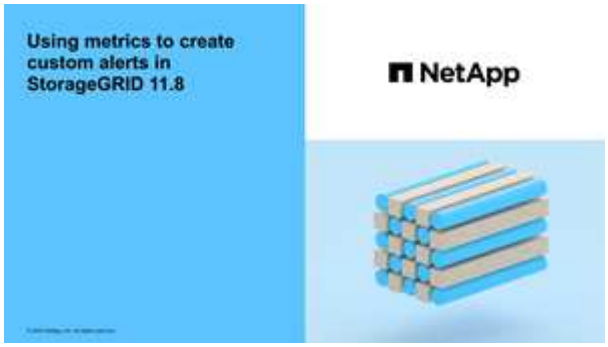
Cabeçalho da coluna	Descrição
Nome	O nome exclusivo e a descrição da regra de alerta. As regras de alerta personalizadas são listadas primeiro, seguidas pelas regras de alerta padrão. O nome da regra de alerta é o assunto das notificações por e-mail.
Condições	As expressões do Prometheus que determinam quando esse alerta é acionado. Um alerta pode ser disparado em um ou mais dos seguintes níveis de gravidade, mas não é necessária uma condição para cada gravidade. • *Crítico* : Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido. • *Principal* : Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID . • *Menor* : O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.
Tipo	O tipo de regra de alerta: • **Padrão**: Uma regra de alerta fornecida com o sistema. Você pode desabilitar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Você não pode remover uma regra de alerta padrão. • **Padrão***: Uma regra de alerta padrão que inclui uma condição ou duração editada. Conforme necessário, você pode facilmente reverter uma condição modificada para o padrão original. • **Personalizado**: Uma regra de alerta que você criou. Você pode desabilitar, editar e remover regras de alerta personalizadas.
Status	Se esta regra de alerta está habilitada ou desabilitada no momento. As condições para regras de alerta desabilitadas não são avaliadas, portanto, nenhum alerta é acionado.

Crie regras de alerta personalizadas

Você pode criar regras de alerta personalizadas para definir suas próprias condições para acionar alertas.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .
- Você está familiarizado com o"métricas Prometheus comumente usadas" .
- Você entende o "sintaxe das consultas do Prometheus" .
- Opcionalmente, você assistiu ao vídeo: "Vídeo: Alertas personalizados" .



Sobre esta tarefa

O StorageGRID não valida alertas personalizados. Se você decidir criar regras de alerta personalizadas, siga estas diretrizes gerais:

- Veja as condições das regras de alerta padrão e use-as como exemplos para suas regras de alerta personalizadas.
- Se você definir mais de uma condição para uma regra de alerta, use a mesma expressão para todas as condições. Em seguida, altere o valor limite para cada condição.
- Verifique cuidadosamente cada condição em busca de erros de digitação e de lógica.
- Use apenas as métricas listadas na API de gerenciamento de grade.
- Ao testar uma expressão usando a API de gerenciamento de grade, esteja ciente de que uma resposta "bem-sucedida" pode ser um corpo de resposta vazio (nenhum alerta acionado). Para ver se o alerta realmente foi acionado, você pode definir temporariamente um limite para um valor que você espera que seja verdadeiro no momento.

  Por exemplo, para testar a expressão `node_memory_MemTotal_bytes < 24000000000` , primeiro execute `node_memory_MemTotal_bytes >= 0` e garantir que você obtenha os resultados esperados (todos os nós retornam um valor). Em seguida, altere o operador e o limite de volta para os valores pretendidos e execute novamente. Nenhum resultado indica que não há alertas atuais para esta expressão.

- Não presuma que um alerta personalizado está funcionando a menos que você tenha validado que o alerta foi disparado quando esperado.

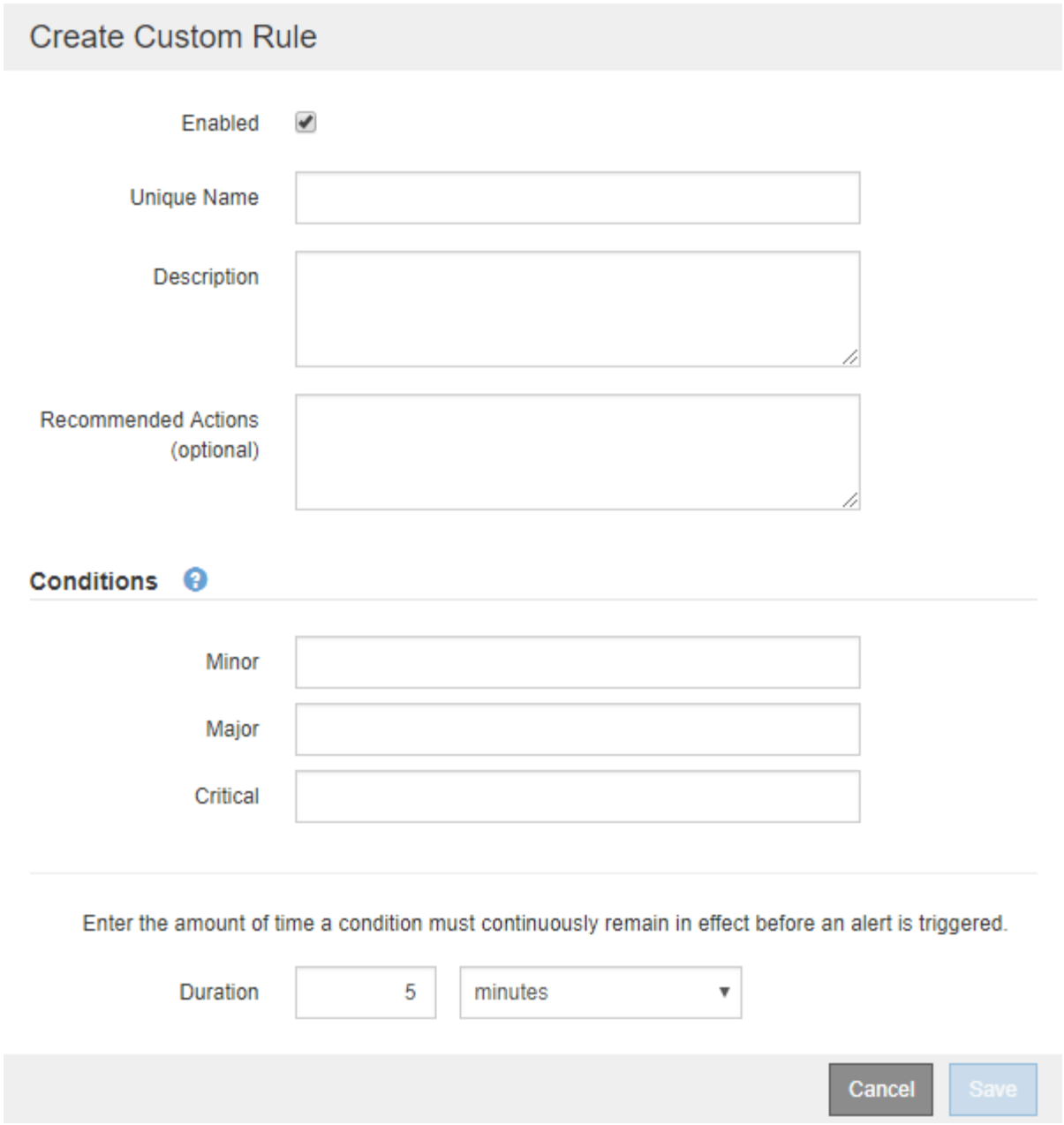
Passos

1. Selecione **ALERTAS** > **Regras**.

   A página Regras de alerta é exibida.

2. Selecione **Criar regra personalizada**.

   A caixa de diálogo Criar regra personalizada é exibida.



3. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no momento.

   Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.

4. Insira as seguintes informações:

Campo	Descrição
Nome Único	Um nome exclusivo para esta regra. O nome da regra de alerta é exibido na página Alertas e também é o assunto das notificações por e-mail. Os nomes das regras de alerta podem ter entre 1 e 64 caracteres.

Campo	Descrição
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta exibida na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 caracteres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando este alerta for acionado. Insira as ações recomendadas como texto simples (sem códigos de formatação). As ações recomendadas para regras de alerta podem ter entre 0 e 1.024 caracteres.

5. Na seção Condições, insira uma expressão do Prometheus para um ou mais níveis de gravidade do alerta.

   Uma expressão básica geralmente tem a forma:

   ```
   [metric] [operator] [value]
   ```

   As expressões podem ter qualquer comprimento, mas aparecem em uma única linha na interface do usuário. Pelo menos uma expressão é necessária.

   Esta expressão faz com que um alerta seja disparado se a quantidade de RAM instalada para um nó for menor que 24.000.000.000 bytes (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Para ver as métricas disponíveis e testar as expressões do Prometheus, selecione o ícone de ajuda e siga o link para a seção Métricas da API de gerenciamento de grade.

6. No campo **Duração**, insira o tempo que uma condição deve permanecer continuamente em vigor antes que o alerta seja acionado e selecione uma unidade de tempo.

   Para acionar um alerta imediatamente quando uma condição se tornar verdadeira, digite **0**. Aumente esse valor para evitar que condições temporárias acionem alertas.

   O padrão é 5 minutos.

7. Selecione **Salvar**.

   A caixa de diálogo é fechada e a nova regra de alerta personalizada aparece na tabela Regras de alerta.

Editar regras de alerta

Você pode editar uma regra de alerta para alterar as condições de acionamento. Para uma regra de alerta personalizada, você também pode atualizar o nome da regra, a descrição e as ações recomendadas.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Sobre esta tarefa

Ao editar uma regra de alerta padrão, você pode alterar as condições para alertas secundários, principais e críticos; e a duração. Ao editar uma regra de alerta personalizada, você também pode editar o nome, a descrição e as ações recomendadas da regra.

> Tenha cuidado ao decidir editar uma regra de alerta. Se você alterar os valores do gatilho, talvez não seja possível detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

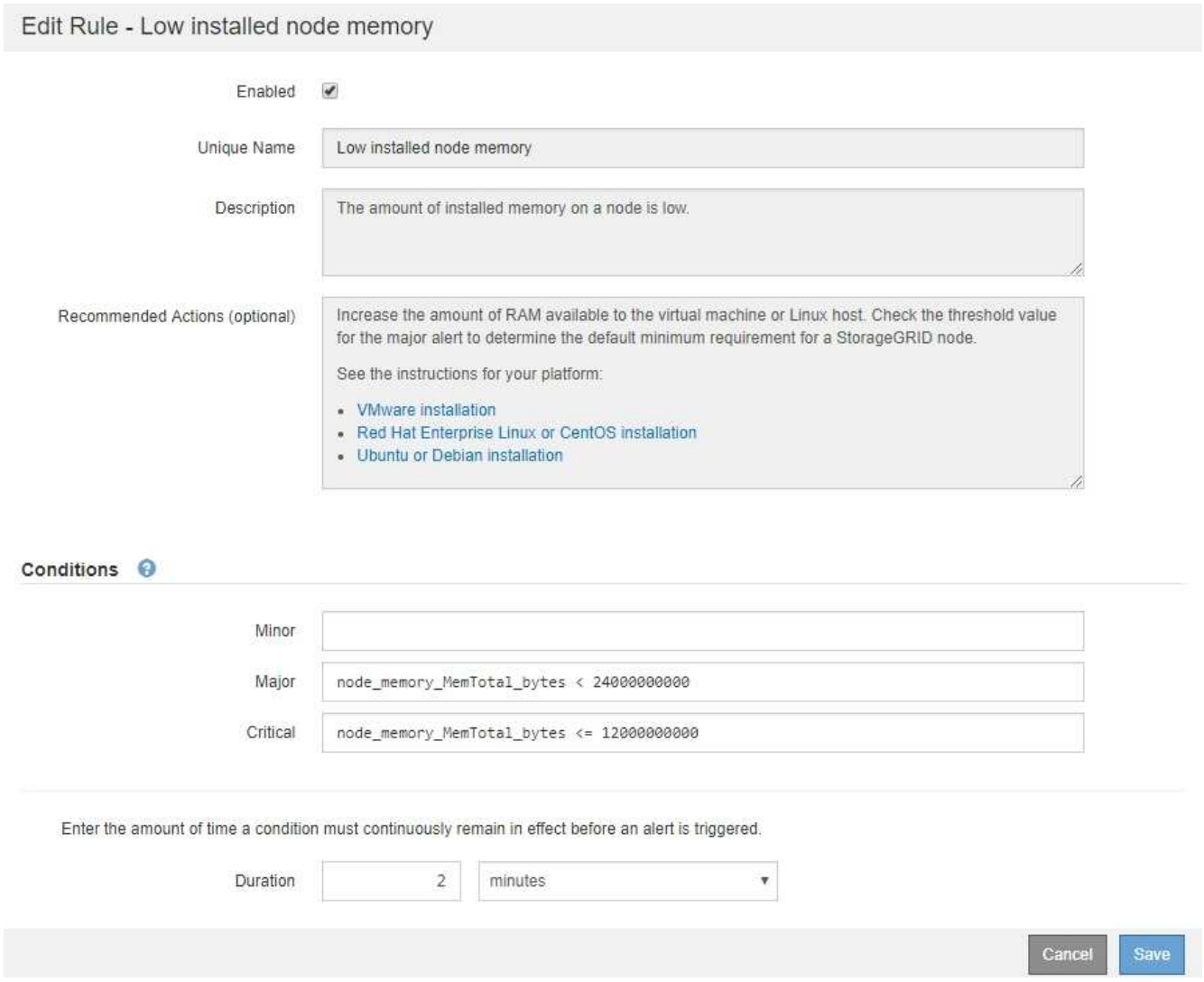
Passos

1. Selecione **ALERTAS** > **Regras**.

   A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta que você deseja editar.
3. Selecione **Editar regra**.

   A caixa de diálogo Editar regra é exibida. Este exemplo mostra uma regra de alerta padrão: os campos Nome exclusivo, Descrição e Ações recomendadas estão desabilitados e não podem ser editados.



4. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no

momento.

Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.

Se você desabilitar a regra de alerta para um alerta atual, deverá aguardar alguns minutos para que o alerta não apareça mais como um alerta ativo.

Em geral, não é recomendado desabilitar uma regra de alerta padrão. Se uma regra de alerta estiver desabilitada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

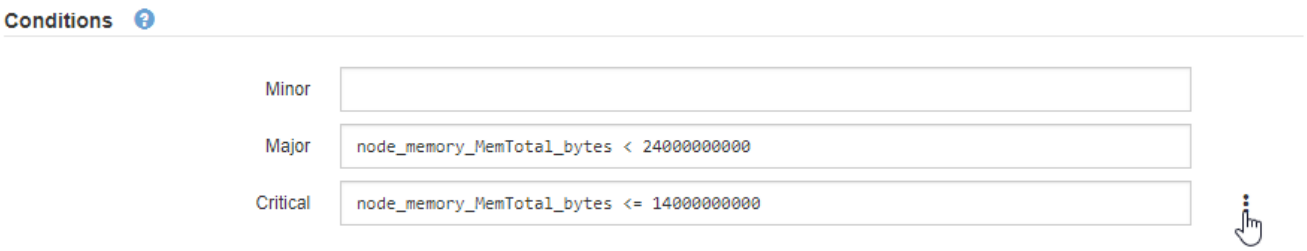
5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.

Você não pode editar essas informações para regras de alerta padrão.

Campo	Descrição
Nome Único	Um nome exclusivo para esta regra. O nome da regra de alerta é exibido na página Alertas e também é o assunto das notificações por e-mail. Os nomes das regras de alerta podem ter entre 1 e 64 caracteres.
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta exibida na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 caracteres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando este alerta for acionado. Insira as ações recomendadas como texto simples (sem códigos de formatação). As ações recomendadas para regras de alerta podem ter entre 0 e 1.024 caracteres.

6. Na seção Condições, insira ou atualize a expressão do Prometheus para um ou mais níveis de gravidade do alerta.

Se você quiser restaurar uma condição de uma regra de alerta padrão editada ao seu valor original, selecione os três pontos à direita da condição modificada.



Se você atualizar as condições de um alerta atual, suas alterações poderão não ser implementadas até que a condição anterior seja resolvida. Na próxima vez que uma das condições da regra for atendida, o alerta refletirá os valores atualizados.

Uma expressão básica geralmente tem a forma:

```
[metric] [operator] [value]
```

As expressões podem ter qualquer comprimento, mas aparecem em uma única linha na interface do usuário. Pelo menos uma expressão é necessária.

Esta expressão faz com que um alerta seja disparado se a quantidade de RAM instalada para um nó for menor que 24.000.000.000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. No campo **Duração**, insira o tempo que uma condição deve permanecer continuamente em vigor antes que o alerta seja acionado e selecione a unidade de tempo.

   Para acionar um alerta imediatamente quando uma condição se tornar verdadeira, digite **0**. Aumente esse valor para evitar que condições temporárias acionem alertas.

   O padrão é 5 minutos.

8. Selecione **Salvar**.

   Se você editou uma regra de alerta padrão, **Padrão*** aparecerá na coluna Tipo. Se você desabilitou uma regra de alerta padrão ou personalizada, **Desabilitado** aparecerá na coluna **Status**.

Desativar regras de alerta

Você pode alterar o estado ativado/desativado de uma regra de alerta padrão ou personalizada.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Sobre esta tarefa

Quando uma regra de alerta é desabilitada, suas expressões não são avaliadas e nenhum alerta é acionado.

Em geral, não é recomendado desabilitar uma regra de alerta padrão. Se uma regra de alerta estiver desabilitada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

1. Selecione **ALERTAS** > **Regras**.

   A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta que você deseja desabilitar ou habilitar.

3. Selecione **Editar regra**.

   A caixa de diálogo Editar regra é exibida.

4. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no momento.

   Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.

   > Se você desabilitar a regra de alerta para um alerta atual, deverá aguardar alguns minutos para que o alerta não seja mais exibido como um alerta ativo.

5. Selecione **Salvar**.

   Desativado aparece na coluna **Status**.

Remover regras de alerta personalizadas

Você pode remover uma regra de alerta personalizada se não quiser mais usá-la.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Passos

1. Selecione **ALERTAS** > **Regras**.

   A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta personalizada que você deseja remover.

   Você não pode remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

   Uma caixa de diálogo de confirmação é exibida.

4. Selecione **OK** para remover a regra de alerta.

   Quaisquer instâncias ativas do alerta serão resolvidas em 10 minutos.

Gerenciar notificações de alerta

Configurar notificações SNMP para alertas

Se quiser que o StorageGRID envie notificações SNMP quando ocorrerem alertas, você deve habilitar o agente SNMP do StorageGRID e configurar um ou mais destinos de interceptação.

Você pode usar a opção **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP** no Grid Manager ou os pontos de extremidade SNMP da Grid Management API para habilitar e configurar o agente SNMP do

StorageGRID . O agente SNMP suporta todas as três versões do protocolo SNMP.

Para aprender a configurar o agente SNMP, consulte"Usar monitoramento SNMP" .

Depois de configurar o agente SNMP do StorageGRID , dois tipos de notificações orientadas a eventos podem ser enviadas:

- Armadilhas são notificações enviadas pelo agente SNMP que não exigem confirmação pelo sistema de gerenciamento. As armadilhas servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como um alerta sendo disparado. As armadilhas são suportadas em todas as três versões do SNMP.
- As informações são semelhantes às armadilhas, mas exigem reconhecimento pelo sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará a informação até que uma confirmação seja recebida ou o valor máximo de novas tentativas seja atingido. As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de captura e informação são enviadas quando um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP de um alerta, você deve configurar um silêncio para o alerta. Ver "Silenciar notificações de alerta" .

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal será o remetente preferencial para notificações de alerta, pacotes de AutoSupport e traps e informações SNMP. Se o nó administrativo principal ficar indisponível, as notificações serão enviadas temporariamente por outros nós administrativos. Ver "O que é um nó de administração?" .

Configurar notificações por e-mail para alertas

Se quiser que notificações por e-mail sejam enviadas quando ocorrerem alertas, você deve fornecer informações sobre seu servidor SMTP. Você também deve inserir os endereços de e-mail dos destinatários das notificações de alerta.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Sobre esta tarefa

A configuração de e-mail usada para notificações de alerta não é usada para pacotes AutoSupport . No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações.

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal será o remetente preferencial para notificações de alerta, pacotes de AutoSupport e traps e informações SNMP. Se o nó administrativo principal ficar indisponível, as notificações serão enviadas temporariamente por outros nós administrativos. Ver "O que é um nó de administração?" .

Passos

1. Selecione **ALERTAS** > **Configuração de e-mail**.

   A página Configuração de e-mail é exibida.

2. Marque a caixa de seleção **Ativar notificações por e-mail** para indicar que você deseja que e-mails de notificação sejam enviados quando os alertas atingirem os limites configurados.

   As seções Servidor de e-mail (SMTP), Segurança da camada de transporte (TLS), Endereços de e-mail e

Filtros são exibidas.

3. Na seção Servidor de e-mail (SMTP), insira as informações que o StorageGRID precisa para acessar seu servidor SMTP.

   Se o seu servidor SMTP exigir autenticação, você deverá fornecer um nome de usuário e uma senha.

Campo	Digitar
Servidor de e-mail	O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor SMTP.
Porta	A porta usada para acessar o servidor SMTP. Deve estar entre 1 e 65535.
Nome de usuário (opcional)	Se o seu servidor SMTP exigir autenticação, insira o nome de usuário para autenticação.
Senha (opcional)	Se o seu servidor SMTP exigir autenticação, digite a senha para autenticação.

4. Na seção Endereços de e-mail, insira os endereços de e-mail do remetente e de cada destinatário.
   a. Para o **Endereço de e-mail do remetente**, especifique um endereço de e-mail válido para usar como endereço De para notificações de alerta.

      Por exemplo: `storagegrid-alerts@example.com`

   b. Na seção Destinatários, insira um endereço de e-mail para cada lista de e-mail ou pessoa que deve receber um e-mail quando ocorrer um alerta.

      Selecione o ícone de mais+ para adicionar destinatários.

5. Se a Segurança da Camada de Transporte (TLS) for necessária para comunicações com o servidor SMTP, selecione **Exigir TLS** na seção Segurança da Camada de Transporte (TLS).
   a. No campo **Certificado CA**, forneça o certificado CA que será usado para verificar a identidade do servidor SMTP.

      Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.

      Você deve fornecer um único arquivo que contenha os certificados de cada autoridade certificadora (CA) emissora intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

   b. Marque a caixa de seleção **Enviar certificado de cliente** se o seu servidor de e-mail SMTP exigir que os remetentes de e-mail forneçam certificados de cliente para autenticação.
   c. No campo **Certificado do cliente**, forneça o certificado do cliente codificado em PEM para enviar ao servidor SMTP.

      Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.

   d. No campo **Chave Privada**, insira a chave privada do certificado do cliente na codificação PEM não

criptografada.

Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.

Se precisar editar a configuração do e-mail, selecione o ícone de lápis para atualizar este campo.

6. Na seção Filtros, selecione quais níveis de gravidade de alerta devem resultar em notificações por e-mail, a menos que a regra para um alerta específico tenha sido silenciada.

Gravidade	Descrição
Menor, maior, crítico	Uma notificação por e-mail é enviada quando a condição menor, maior ou crítica de uma regra de alerta é atendida.
Importante, crítico	Uma notificação por e-mail é enviada quando a condição principal ou crítica para uma regra de alerta é atendida. Notificações não são enviadas para alertas menores.
Somente crítico	Uma notificação por e-mail é enviada somente quando a condição crítica para uma regra de alerta é atendida. Notificações não são enviadas para alertas menores ou maiores.

7. Quando estiver pronto para testar suas configurações de e-mail, execute estas etapas:
   a. Selecione **Enviar e-mail de teste**.

      Uma mensagem de confirmação é exibida, indicando que um e-mail de teste foi enviado.

   b. Verifique as caixas de entrada de todos os destinatários de e-mail e confirme se um e-mail de teste foi recebido.

      Se o e-mail não for recebido em alguns minutos ou se o alerta **Falha na notificação por e-mail** for acionado, verifique suas configurações e tente novamente.

   c. Sign in em qualquer outro nó de administração e envie um e-mail de teste para verificar a conectividade de todos os sites.

      Ao testar notificações de alerta, você deve fazer login em cada nó de administração para verificar a conectividade. Isso contrasta com o teste de pacotes do AutoSupport , em que todos os nós administrativos enviam o e-mail de teste.

8. Selecione **Salvar**.

   O envio de um e-mail de teste não salva suas configurações. Você deve selecionar **Salvar**.

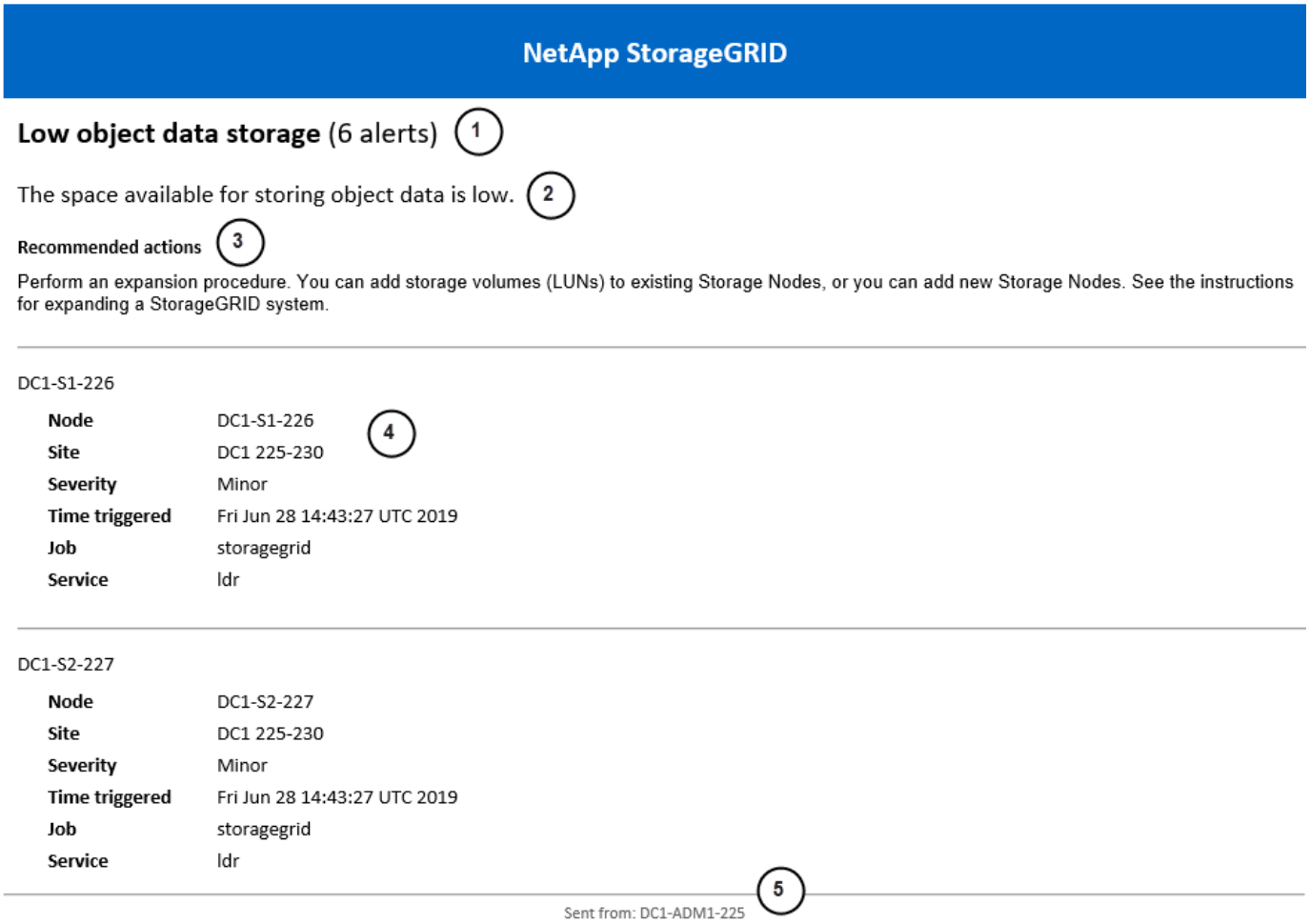
   As configurações de e-mail são salvas.

Informações incluídas nas notificações de alerta por e-mail

Após configurar o servidor de e-mail SMTP, notificações por e-mail serão enviadas aos destinatários designados quando um alerta for acionado, a menos que a regra de alerta seja suprimida por um silêncio. Ver

"Silenciar notificações de alerta" .

As notificações por e-mail incluem as seguintes informações:



Chamar	Descrição
1	O nome do alerta, seguido pelo número de instâncias ativas deste alerta.
2	A descrição do alerta.
3	Quaisquer ações recomendadas para o alerta.
4	Detalhes sobre cada instância ativa do alerta, incluindo o nó e o site afetados, a gravidade do alerta, o horário UTC em que a regra de alerta foi acionada e o nome do trabalho e serviço afetados.
5	O nome do host do nó de administração que enviou a notificação.

Como os alertas são agrupados

Para evitar que um número excessivo de notificações por e-mail seja enviado quando os alertas são acionados, o StorageGRID tenta agrupar vários alertas na mesma notificação.

Consulte a tabela a seguir para obter exemplos de como o StorageGRID agrupa vários alertas em notificações por e-mail.

Comportamento	Exemplo
Cada notificação de alerta se aplica somente a alertas que tenham o mesmo nome. Se dois alertas com nomes diferentes forem disparados ao mesmo tempo, duas notificações por e-mail serão enviadas.	• O alerta A é acionado em dois nós ao mesmo tempo. Apenas uma notificação é enviada. • O alerta A é acionado no nó 1 e o alerta B é acionado no nó 2 ao mesmo tempo. Duas notificações são enviadas — uma para cada alerta.
Para um alerta específico em um nó específico, se os limites forem atingidos para mais de uma gravidade, uma notificação será enviada apenas para o alerta mais grave.	• O alerta A é acionado e os limites de alerta menor, maior e crítico são atingidos. Uma notificação é enviada para o alerta crítico.
Na primeira vez que um alerta é disparado, o StorageGRID aguarda 2 minutos antes de enviar uma notificação. Se outros alertas com o mesmo nome forem acionados durante esse período, o StorageGRID agrupará todos os alertas na notificação inicial.	1. O alerta A é acionado no nó 1 às 08:00. Nenhuma notificação é enviada. 2. O alerta A é acionado no nó 2 às 08:01. Nenhuma notificação é enviada. 3. Às 08:02, uma notificação é enviada para relatar ambas as instâncias do alerta.
Se outro alerta com o mesmo nome for acionado, o StorageGRID aguardará 10 minutos antes de enviar uma nova notificação. A nova notificação relata todos os alertas ativos (alertas atuais que não foram silenciados), mesmo que tenham sido relatados anteriormente.	1. O alerta A é acionado no nó 1 às 08:00. Uma notificação é enviada às 08:02. 2. O alerta A é acionado no nó 2 às 08:05. Uma segunda notificação é enviada às 08:15 (10 minutos depois). Ambos os nós são relatados.
Se houver vários alertas atuais com o mesmo nome e um deles for resolvido, uma nova notificação não será enviada se o alerta ocorrer novamente no nó para o qual o alerta foi resolvido.	1. O alerta A é acionado para o nó 1. Uma notificação é enviada. 2. O alerta A é acionado para o nó 2. Uma segunda notificação é enviada. 3. O alerta A é resolvido para o nó 2, mas permanece ativo para o nó 1. 4. O alerta A é acionado novamente para o nó 2. Nenhuma nova notificação é enviada porque o alerta ainda está ativo para o nó 1.
O StorageGRID continua enviando notificações por e-mail uma vez a cada 7 dias até que todas as instâncias do alerta sejam resolvidas ou a regra de alerta seja silenciada.	1. O alerta A é acionado para o nó 1 em 8 de março. Uma notificação é enviada. 2. O alerta A não foi resolvido nem silenciado. Notificações adicionais são enviadas em 15 de março, 22 de março, 29 de março e assim por diante.

Solucionar problemas de notificações de alerta por e-mail

Se o alerta **Falha na notificação por e-mail** for acionado ou você não conseguir receber a notificação por e-mail de alerta de teste, siga estas etapas para resolver o problema.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Passos

1. Verifique suas configurações.
   a. Selecione **ALERTAS** > **Configuração de e-mail**.
   b. Verifique se as configurações do servidor de e-mail (SMTP) estão corretas.
   c. Verifique se você especificou endereços de e-mail válidos para os destinatários.
2. Verifique seu filtro de spam e certifique-se de que o e-mail não foi enviado para uma pasta de lixo eletrônico.
3. Peça ao seu administrador de e-mail para confirmar se os e-mails do endereço do remetente não estão sendo bloqueados.
4. Colete um arquivo de log para o nó de administração e entre em contato com o suporte técnico.

   O suporte técnico pode usar as informações nos logs para ajudar a determinar o que deu errado. Por exemplo, o arquivo prometheus.log pode mostrar um erro ao conectar-se ao servidor especificado.

   Ver "Coletar arquivos de log e dados do sistema" .

Silenciar notificações de alerta

Opcionalmente, você pode configurar silêncios para suprimir temporariamente notificações de alerta.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Gerenciar alertas ou permissão de acesso root" .

Sobre esta tarefa

Você pode silenciar regras de alerta em toda a grade, em um único site ou em um único nó e para uma ou mais severidades. Cada silêncio suprime todas as notificações para uma única regra de alerta ou para todas as regras de alerta.

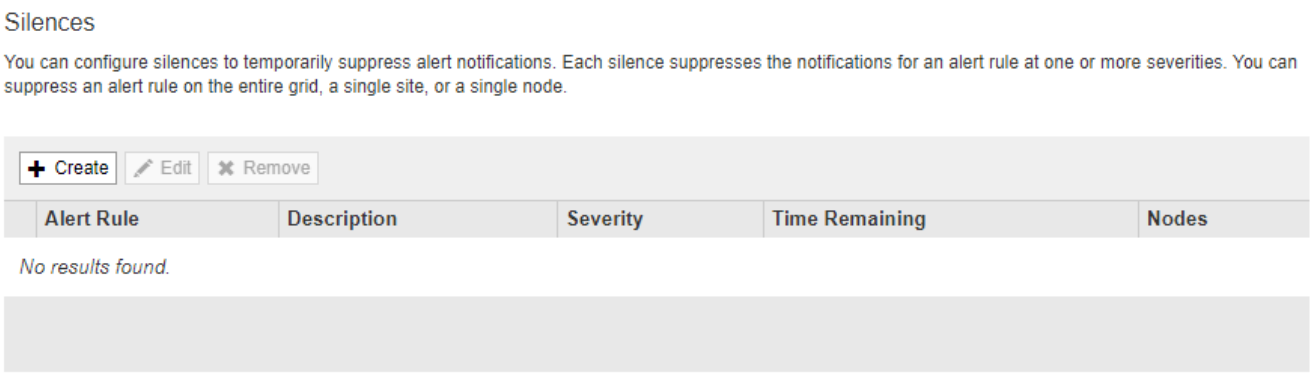
Se você tiver habilitado o agente SNMP, os silêncios também suprimem as interceptações e informações SNMP.

> Tenha cuidado ao decidir silenciar uma regra de alerta. Se você silenciar um alerta, poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

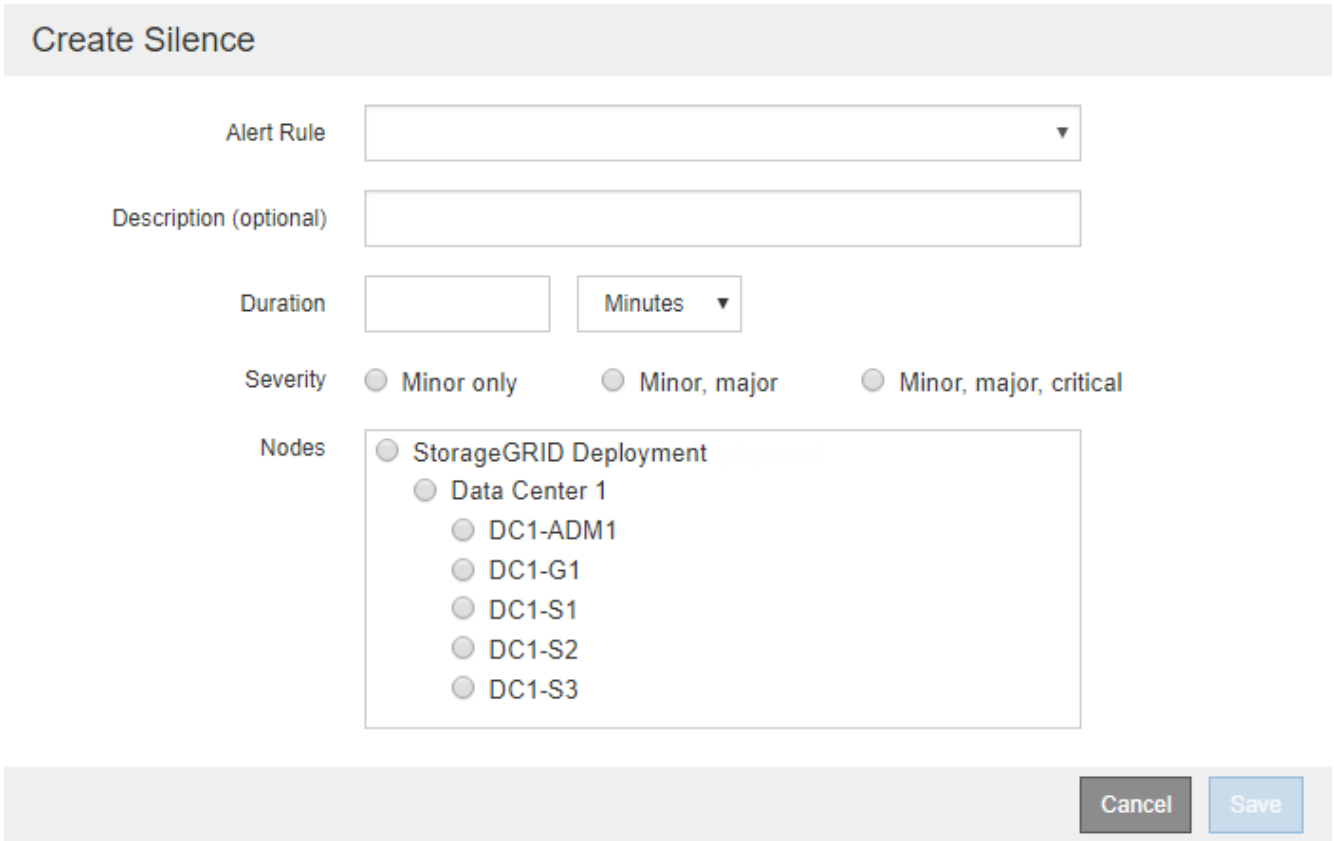
1. Selecione **ALERTAS** > **Silêncios**.

   A página Silêncios é exibida.



2. Selecione **Criar**.

   A caixa de diálogo Criar Silêncio é exibida.



3. Selecione ou insira as seguintes informações:

Campo	Descrição
Regra de Alerta	O nome da regra de alerta que você deseja silenciar. Você pode selecionar qualquer regra de alerta padrão ou personalizada, mesmo que a regra de alerta esteja desabilitada. **Observação:** Selecione **Todas as regras** se quiser silenciar todas as regras de alerta usando os critérios especificados nesta caixa de diálogo.

Campo	Descrição
Descrição	Opcionalmente, uma descrição do silêncio. Por exemplo, descreva o propósito desse silêncio.
Duração	Por quanto tempo você quer que esse silêncio permaneça em vigor, em minutos, horas ou dias. O silêncio pode vigorar de 5 minutos a 1.825 dias (5 anos). **Observação:** você não deve silenciar uma regra de alerta por um longo período de tempo. Se uma regra de alerta for silenciada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica. No entanto, pode ser necessário usar um silêncio prolongado se um alerta for disparado por uma configuração específica e intencional, como pode ser o caso dos alertas **Link do dispositivo de serviços inativo** e **Link do dispositivo de armazenamento inativo**.
Gravidade	Qual(is) gravidade(s) de alerta deve(m) ser silenciada(s). Se o alerta for disparado em uma das gravidades selecionadas, nenhuma notificação será enviada.
Nós	A qual nó ou nós você deseja que esse silêncio seja aplicado. Você pode suprimir uma regra de alerta ou todas as regras na grade inteira, em um único site ou em um único nó. Se você selecionar a grade inteira, o silêncio será aplicado a todos os sites e todos os nós. Se você selecionar um site, o silêncio se aplicará somente aos nós naquele site. **Observação:** você não pode selecionar mais de um nó ou mais de um site para cada silêncio. Você deve criar silêncios adicionais se quiser suprimir a mesma regra de alerta em mais de um nó ou mais de um site ao mesmo tempo.

4. Selecione **Salvar**.
5. Se quiser modificar ou encerrar um silêncio antes que ele expire, você pode editá-lo ou removê-lo.

Opção	Descrição
Editar um silêncio	a. Selecione **ALERTAS** > **Silêncios**. b. Na tabela, selecione o botão de opção para o silêncio que você deseja editar. c. Selecione **Editar**. d. Altere a descrição, o tempo restante, as gravidades selecionadas ou o nó afetado. e. Selecione **Salvar**.

Opção	Descrição
Remover um silêncio	a. Selecione **ALERTAS** > **Silêncios**. b. Na tabela, selecione o botão de opção para o silêncio que você deseja remover. c. Selecione **Remover**. d. Selecione **OK** para confirmar que deseja remover esse silêncio. **Observação**: agora as notificações serão enviadas quando este alerta for acionado (a menos que seja suprimido por outro silêncio). Se este alerta estiver acionado no momento, pode levar alguns minutos para que as notificações por e-mail ou SNMP sejam enviadas e para que a página Alertas seja atualizada.

Informações relacionadas

"Configurar o agente SNMP"

Referência de alertas

Esta referência lista os alertas padrão que aparecem no Grid Manager. As ações recomendadas estão na mensagem de alerta que você recebe.

Conforme necessário, você pode criar regras de alerta personalizadas para se adequar à sua abordagem de gerenciamento de sistema.

Alguns dos alertas padrão usam"Métricas do Prometheus" .

Alertas de aparelhos

Nome do alerta	Descrição
Bateria do aparelho vencida	A bateria no controlador de armazenamento do aparelho expirou.
A bateria do aparelho falhou	A bateria no controlador de armazenamento do aparelho falhou.
A bateria do aparelho tem capacidade de aprendizagem insuficiente	A bateria no controlador de armazenamento do aparelho não tem capacidade de aprendizagem suficiente.
Bateria do aparelho próxima da validade	A bateria no controlador de armazenamento do aparelho está quase acabando.
Bateria do aparelho removida	A bateria no controlador de armazenamento do aparelho está faltando.
Bateria do aparelho muito quente	A bateria no controlador de armazenamento do aparelho está superaquecida.

Nome do alerta	Descrição
Erro de comunicação BMC do aparelho	A comunicação com o controlador de gerenciamento da placa de base (BMC) foi perdida.
Falha detectada no dispositivo de inicialização do aparelho	Foi detectado um problema com o dispositivo de inicialização no dispositivo.
Falha no dispositivo de backup do cache do aparelho	Um dispositivo de backup de cache persistente falhou.
Capacidade insuficiente do dispositivo de backup de cache do aparelho	Não há capacidade suficiente no dispositivo de backup de cache.
Dispositivo de backup de cache do aparelho protegido contra gravação	Um dispositivo de backup de cache é protegido contra gravação.
Incompatibilidade de tamanho de memória cache do dispositivo	Os dois controladores no dispositivo têm tamanhos de cache diferentes.
Falha na bateria do CMOS do aparelho	Foi detectado um problema com a bateria CMOS do aparelho.
Temperatura do chassi do controlador de computação do dispositivo muito alta	A temperatura do controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.
Temperatura da CPU do controlador de computação do dispositivo muito alta	A temperatura da CPU no controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.
O controlador de computação do dispositivo precisa de atenção	Uma falha de hardware foi detectada no controlador de computação de um dispositivo StorageGRID .
A fonte de alimentação do controlador de computação do aparelho A tem um problema	A fonte de alimentação A no controlador de computação tem um problema.
A fonte de alimentação do controlador de computação do aparelho B tem um problema	A fonte de alimentação B no controlador de computação tem um problema.
O serviço de monitoramento de hardware de computação do dispositivo foi interrompido	O serviço que monitora o status do hardware de armazenamento parou.

Nome do alerta	Descrição
Unidade DAS do dispositivo excedendo o limite de dados gravados por dia	Uma quantidade excessiva de dados está sendo gravada em uma unidade todos os dias, o que pode anular sua garantia.
Falha detectada na unidade DAS do aparelho	Um problema foi detectado com uma unidade de armazenamento de conexão direta (DAS) no dispositivo.
Luz localizadora do acionamento DAS do aparelho acesa	A luz do localizador de unidade para uma ou mais unidades de armazenamento de conexão direta (DAS) em um nó de armazenamento do dispositivo está acesa.
Reconstrução da unidade DAS do aparelho	Uma unidade de armazenamento de conexão direta (DAS) está sendo reconstruída. Isso é esperado se ele foi substituído ou removido/reinserida recentemente.
Falha detectada no ventilador do aparelho	Foi detectado um problema com uma unidade de ventilação do aparelho.
Falha de canal de fibra do aparelho detectada	Um problema de link Fibre Channel foi detectado entre o controlador de armazenamento do dispositivo e o controlador de computação
Falha na porta HBA do Fibre Channel do aparelho	Uma porta HBA Fibre Channel está falhando ou falhou.
Unidades de cache flash do dispositivo não são ideais	As unidades usadas para o cache SSD não são ideais.
Interconexão do aparelho/recipiente da bateria removido	O compartimento de interconexão/bateria está faltando.
Porta LACP do aparelho ausente	Uma porta em um dispositivo StorageGRID não está participando do vínculo LACP.
Falha na placa de rede do dispositivo detectada	Foi detectado um problema com uma placa de interface de rede (NIC) no dispositivo.
O fornecimento geral de energia do aparelho está degradado	A alimentação de um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
Aviso crítico de SSD do aparelho	Um SSD de dispositivo está relatando um aviso crítico.
Falha do controlador de armazenamento do dispositivo A	O controlador de armazenamento A em um dispositivo StorageGRID falhou.

Nome do alerta	Descrição
Falha do controlador de armazenamento do aparelho B	O controlador de armazenamento B em um dispositivo StorageGRID falhou.
Falha na unidade do controlador de armazenamento do dispositivo	Uma ou mais unidades em um dispositivo StorageGRID falharam ou não estão ideais.
Problema de hardware do controlador de armazenamento do dispositivo	O software SANtricity está relatando "Precisa de atenção" para um componente em um dispositivo StorageGRID .
Falha na fonte de alimentação A do controlador de armazenamento do aparelho	A fonte de alimentação A em um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
Falha na fonte de alimentação B do controlador de armazenamento do aparelho	A fonte de alimentação B em um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
O serviço de monitoramento de hardware de armazenamento do dispositivo foi interrompido	O serviço que monitora o status do hardware de armazenamento parou.
Prateleiras de armazenamento de eletrodomésticos degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento está degradado.
Temperatura do aparelho excedida	A temperatura nominal ou máxima do controlador de armazenamento do aparelho foi excedida.
Sensor de temperatura do aparelho removido	Um sensor de temperatura foi removido.
Erro de inicialização segura UEFI do dispositivo	Um dispositivo não foi inicializado com segurança.
A E/S do disco é muito lenta	E/S de disco muito lentas podem estar afetando o desempenho da grade.
Falha detectada no ventilador do aparelho de armazenamento	Foi detectado um problema com uma unidade de ventilador no controlador de armazenamento de um aparelho.
Conectividade de armazenamento do dispositivo de armazenamento degradada	Há um problema com uma ou mais conexões entre o controlador de computação e o controlador de armazenamento.
Dispositivo de armazenamento inacessível	Não é possível acessar um dispositivo de armazenamento.

Alertas de auditoria e syslog

Nome do alerta	Descrição
Os logs de auditoria estão sendo adicionados à fila na memória	O nó não pode enviar logs para o servidor syslog local e a fila na memória está ficando cheia.
Erro de encaminhamento do servidor syslog externo	O nó não pode encaminhar logs para o servidor syslog externo.
Grande fila de auditoria	A fila de disco para mensagens de auditoria está cheia. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Os logs estão sendo adicionados à fila no disco	O nó não pode encaminhar logs para o servidor syslog externo e a fila no disco está ficando cheia.

Alertas de balde

Nome do alerta	Descrição
O bucket FabricPool tem uma configuração de consistência de bucket não suportada	Um bucket FabricPool usa o nível de consistência Available ou Strong-site, que não é suportado.
O bucket FabricPool tem uma configuração de controle de versão não suportada	Um bucket FabricPool tem controle de versão ou bloqueio de objeto S3 habilitado, que não são suportados.

Alertas de Cassandra

Nome do alerta	Descrição
Erro do compactador automático do Cassandra	Ocorreu um erro no compactador automático Cassandra.
Métricas do compactador automático Cassandra desatualizadas	As métricas que descrevem o autocompactador Cassandra estão desatualizadas.
Erro de comunicação do Cassandra	Os nós que executam o serviço Cassandra estão tendo problemas para se comunicar entre si.
Compactações de Cassandra sobrecarregadas	O processo de compactação do Cassandra está sobrecarregado.
Erro de gravação de tamanho excessivo do Cassandra	Um processo interno do StorageGRID enviou uma solicitação de gravação ao Cassandra que era muito grande.

Nome do alerta	Descrição
Métricas de reparo do Cassandra desatualizadas	As métricas que descrevem os trabalhos de reparo do Cassandra estão desatualizadas.
Progresso lento no reparo do Cassandra	O progresso dos reparos do banco de dados Cassandra é lento.
Serviço de reparo Cassandra não disponível	O serviço de reparo do Cassandra não está disponível.
Corrupção da tabela Cassandra	Cassandra detectou corrupção de tabela. O Cassandra reinicia automaticamente se detectar corrupção de tabela.

Alertas do Cloud Storage Pool

Nome do alerta	Descrição
Erro de conectividade do Cloud Storage Pool	A verificação de integridade dos pools de armazenamento em nuvem detectou um ou mais novos erros.
Expiração da certificação de entidade final do IAM Roles Anywhere	O certificado de entidade final do IAM Roles Anywhere está prestes a expirar.

Alertas de replicação entre grades

Nome do alerta	Descrição
Falha permanente na replicação entre redes	Ocorreu um erro de replicação entre grades que requer intervenção do usuário para ser resolvido.
Recursos de replicação entre redes indisponíveis	Solicitações de replicação entre grades estão pendentes porque um recurso não está disponível.

Alertas DHCP

Nome do alerta	Descrição
Concessão de DHCP expirada	O contrato de concessão de DHCP em uma interface de rede expirou.
Concessão de DHCP expirando em breve	O contrato de concessão de DHCP em uma interface de rede expirará em breve.
Servidor DHCP indisponível	O servidor DHCP não está disponível.

Alertas de depuração e rastreamento

Nome do alerta	Descrição
Impacto no desempenho da depuração	Quando o modo de depuração está ativado, o desempenho do sistema pode ser afetado negativamente.
Configuração de rastreamento habilitada	Quando a configuração de rastreamento está ativada, o desempenho do sistema pode ser afetado negativamente.

Alertas de e-mail e AutoSupport

Nome do alerta	Descrição
Falha ao enviar a mensagem do AutoSupport	A mensagem mais recente do AutoSupport falhou ao ser enviada.
Falha na resolução do nome de domínio	O nó StorageGRID não conseguiu resolver nomes de domínio.
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail de um alerta.
Erros de informação SNMP	Erros ao enviar notificações de informação SNMP para um destino de interceptação.
Login SSH ou console detectado	Nas últimas 24 horas, um usuário fez login com o Web Console ou SSH.

Alertas de codificação de apagamento (EC)

Nome do alerta	Descrição
Falha de rebalanceamento da CE	O procedimento de rebalanceamento da CE falhou ou foi interrompido.
Falha no reparo da CE	Um trabalho de reparo para dados EC falhou ou foi interrompido.
Reparo da CE paralisado	Um trabalho de reparo de dados da CE foi interrompido.
Erro de verificação de fragmento codificado por apagamento	Fragmentos codificados por apagamento não podem mais ser verificados. Fragmentos corrompidos podem não ser reparados.

Alertas de expiração de certificados

Nome do alerta	Descrição
Expiração do certificado CA do Proxy de Administração	Um ou mais certificados no pacote de CA do servidor proxy de administração estão prestes a expirar.
Expiração do certificado do cliente	Um ou mais certificados de cliente estão prestes a expirar.

Nome do alerta	Descrição
Expiração do certificado global do servidor para S3 e Swift	O certificado do servidor global para S3 e Swift está prestes a expirar.
Expiração do certificado de ponto de extremidade do balanceador de carga	Um ou mais certificados de ponto de extremidade do balanceador de carga estão prestes a expirar.
Expiração do certificado do servidor para interface de gerenciamento	O certificado do servidor usado para a interface de gerenciamento está prestes a expirar.
Expiração do certificado CA do syslog externo	O certificado da autoridade de certificação (CA) usado para assinar o certificado do servidor syslog externo está prestes a expirar.
Expiração do certificado do cliente syslog externo	O certificado do cliente para um servidor syslog externo está prestes a expirar.
Expiração do certificado do servidor syslog externo	O certificado do servidor apresentado pelo servidor syslog externo está prestes a expirar.

Alertas de rede de grade

Nome do alerta	Descrição
Incompatibilidade de MTU da rede de grade	A configuração de MTU para a interface da rede Grid (eth0) difere significativamente entre os nós da grade.

Alertas de federação de rede

Nome do alerta	Descrição
Expiração do certificado de federação de rede	Um ou mais certificados de federação de rede estão prestes a expirar.
Falha na conexão da federação de rede	A conexão da federação de rede entre a rede local e a remota não está funcionando.

Alertas de alto uso ou alta latência

Nome do alerta	Descrição
Alto uso de heap Java	Uma alta porcentagem do espaço de heap do Java está sendo usada.
Alta latência para consultas de metadados	O tempo médio para consultas de metadados do Cassandra é muito longo.

Alertas de federação de identidade

Nome do alerta	Descrição
Falha na sincronização da federação de identidade	Não é possível sincronizar grupos federados e usuários da fonte de identidade.
Falha na sincronização da federação de identidade para um locatário	Não é possível sincronizar grupos federados e usuários da fonte de identidade configurada por um locatário.

Alertas de gerenciamento do ciclo de vida da informação (ILM)

Nome do alerta	Descrição
Posicionamento ILM inatingível	Uma instrução de posicionamento em uma regra ILM não pode ser obtida para determinados objetos.
Taxa de varredura ILM baixa	A taxa de varredura do ILM está definida para menos de 100 objetos/segundo.

Alertas do servidor de gerenciamento de chaves (KMS)

Nome do alerta	Descrição
Expiração do certificado KMS CA	O certificado da autoridade de certificação (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Expiração do certificado do cliente KMS	O certificado do cliente para um servidor de gerenciamento de chaves está prestes a expirar
Falha ao carregar a configuração do KMS	A configuração do servidor de gerenciamento de chaves existe, mas falhou ao carregar.
Erro de conectividade do KMS	Um nó do dispositivo não pôde se conectar ao servidor de gerenciamento de chaves do seu site.
Nome da chave de criptografia KMS não encontrado	O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido.
Falha na rotação da chave de criptografia do KMS	Todos os volumes do dispositivo foram descriptografados com sucesso, mas um ou mais volumes não puderam ser girados para a chave mais recente.
O KMS não está configurado	Não existe nenhum servidor de gerenciamento de chaves para este site.

Nome do alerta	Descrição
A chave KMS falhou ao descriptografar um volume do dispositivo	Um ou mais volumes em um dispositivo com criptografia de nó habilitada não puderam ser descriptografados com a chave KMS atual.
Expiração do certificado do servidor KMS	O certificado do servidor usado pelo servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Falha de conectividade do servidor KMS	Um nó do dispositivo não pôde se conectar a um ou mais servidores no cluster do servidor de gerenciamento de chaves do seu site.

Alertas do balanceador de carga

Nome do alerta	Descrição
Conexões elevadas do balanceador de carga de solicitação zero	Uma porcentagem elevada de conexões com endpoints do balanceador de carga foram desconectadas sem executar solicitações.

Alertas de deslocamento do relógio local

Nome do alerta	Descrição
Grande deslocamento de tempo do relógio local	O deslocamento entre o relógio local e o horário do Protocolo de Tempo de Rede (NTP) é muito grande.

Alertas de pouca memória ou pouco espaço

Nome do alerta	Descrição
Baixa capacidade do disco de log de auditoria	O espaço disponível para logs de auditoria é baixo. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Memória de nó baixa disponível	A quantidade de RAM disponível em um nó é baixa.
Pouco espaço livre para pool de armazenamento	O espaço disponível para armazenar dados de objetos no Nó de Armazenamento é baixo.
Baixa memória de nó instalada	A quantidade de memória instalada em um nó é baixa.
Baixo armazenamento de metadados	O espaço disponível para armazenar metadados de objetos é baixo.
Baixa capacidade de disco de métricas	O espaço disponível para o banco de dados de métricas é baixo.

Nome do alerta	Descrição
Armazenamento de dados de objetos baixos	O espaço disponível para armazenar dados de objetos é baixo.
Substituição de marca d'água somente leitura	A substituição da marca d'água somente leitura do volume de armazenamento é menor que a marca d'água otimizada mínima para um nó de armazenamento.
Baixa capacidade do disco raiz	O espaço disponível no disco raiz é baixo.
Baixa capacidade de dados do sistema	O espaço disponível para /var/local é baixo. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Pouco espaço livre no diretório tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de nó ou rede de nó

Nome do alerta	Descrição
Uso de recebimento da rede de administração	O uso de recebimento na Rede de Administração é alto.
Uso de transmissão da rede de administração	O uso de transmissão na rede de administração é alto.
Falha na configuração do firewall	Falha ao aplicar a configuração do firewall.
Pontos de extremidade da interface de gerenciamento em modo de fallback	Todos os pontos de extremidade da interface de gerenciamento estão retornando às portas padrão há muito tempo.
Erro de conectividade de rede do nó	Ocorreram erros durante a transferência de dados entre nós.
Erro de quadro de recepção de rede de nó	Uma alta porcentagem dos quadros de rede recebidos por um nó continham erros.
Nó não sincronizado com o servidor NTP	O nó não está sincronizado com o servidor de protocolo de tempo de rede (NTP).
Nó não bloqueado com servidor NTP	O nó não está bloqueado em um servidor de protocolo de tempo de rede (NTP).
Rede de nós não pertencentes ao dispositivo inoperante	Um ou mais dispositivos de rede estão inativos ou desconectados.

Nome do alerta	Descrição
Link do dispositivo de serviços inativo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desconectada.
O link do dispositivo de serviços está inativo na porta 1 da rede de administração	A porta 1 da rede de administração no dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desconectada.
O link do dispositivo de serviços está inativo na porta de rede 1	A porta de rede 1 no dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 2	A porta de rede 2 do dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 3	A porta de rede 3 do dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 4	A porta de rede 4 do dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta 1 da rede de administração	A porta 1 da rede de administração no dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 1	A porta de rede 1 no dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 2	A porta de rede 2 do dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 3	A porta de rede 3 do dispositivo está inativa ou desconectada.

Nome do alerta	Descrição
Link do dispositivo de armazenamento inativo na porta de rede 4	A porta de rede 4 do dispositivo está inativa ou desconectada.
Nó de armazenamento não está no estado de armazenamento desejado	O serviço LDR em um nó de armazenamento não pode fazer a transição para o estado desejado devido a um erro interno ou problema relacionado ao volume
Uso da conexão TCP	O número de conexões TCP neste nó está se aproximando do número máximo que pode ser rastreado.
Não é possível comunicar com o nó	Um ou mais serviços não respondem ou o nó não pode ser alcançado.
Reinicialização inesperada do nó	Um nó foi reinicializado inesperadamente nas últimas 24 horas.

Alertas de objetos

Nome do alerta	Descrição
Falha na verificação de existência do objeto	A tarefa de verificação da existência do objeto falhou.
Verificação de existência de objeto paralisada	O trabalho de verificação de existência do objeto foi interrompido.
Objetos perdidos	Um ou mais objetos foram perdidos da grade.
Tamanho do objeto S3 PUT muito grande	Um cliente está tentando uma operação PUT Object que excede os limites de tamanho do S3.
Objeto corrompido não identificado detectado	Foi encontrado um arquivo no armazenamento de objetos replicados que não pôde ser identificado como um objeto replicado.

Alertas de serviços de plataforma

Nome do alerta	Descrição
Capacidade de solicitação pendente dos Serviços de Plataforma baixa	O número de solicitações pendentes dos Serviços de Plataforma está se aproximando da capacidade.
Serviços de plataforma indisponíveis	Poucos nós de armazenamento com o serviço RSM estão em execução ou disponíveis em um site.

Alertas de volume de armazenamento

Nome do alerta	Descrição
O volume de armazenamento precisa de atenção	Um volume de armazenamento está offline e precisa de atenção.
O volume de armazenamento precisa ser restaurado	Um volume de armazenamento foi recuperado e precisa ser restaurado.
Volume de armazenamento offline	Um volume de armazenamento ficou offline por mais de 5 minutos.
Tentativa de remontagem do volume de armazenamento	Um volume de armazenamento estava offline e acionou uma remontagem automática. Isso pode indicar um problema na unidade ou erros no sistema de arquivos.
A restauração de volume falhou ao iniciar o reparo de dados replicados	O reparo de dados replicados para um volume reparado não pôde ser iniciado automaticamente.

Alertas de serviços do StorageGRID

Nome do alerta	Descrição
serviço nginx usando configuração de backup	A configuração do serviço nginx é inválida. A configuração anterior agora está sendo usada.
serviço nginx-gw usando configuração de backup	A configuração do serviço nginx-gw é inválida. A configuração anterior agora está sendo usada.
Reinicialização necessária para desabilitar o FIPS	A política de segurança não requer o modo FIPS, mas o Módulo de Segurança Criptográfica NetApp está habilitado.
Reinicialização necessária para habilitar o FIPS	A política de segurança requer o modo FIPS, mas o Módulo de Segurança Criptográfica NetApp está desabilitado.
Serviço SSH usando configuração de backup	A configuração do serviço SSH é inválida. A configuração anterior agora está sendo usada.

Alertas de inquilinos

Nome do alerta	Descrição
Uso de cota de inquilino alto	Uma alta porcentagem do espaço de cota está sendo usada. Esta regra está desabilitada por padrão porque pode causar muitas notificações.

Métricas do Prometheus comumente usadas

Consulte esta lista de métricas do Prometheus comumente usadas para entender melhor as condições nas regras de alerta padrão ou para construir as condições para regras de alerta personalizadas.

Você também pode obter uma lista completa de todas as métricas .

Para obter detalhes sobre a sintaxe das consultas do Prometheus, consulte "Consultando Prometeu" .

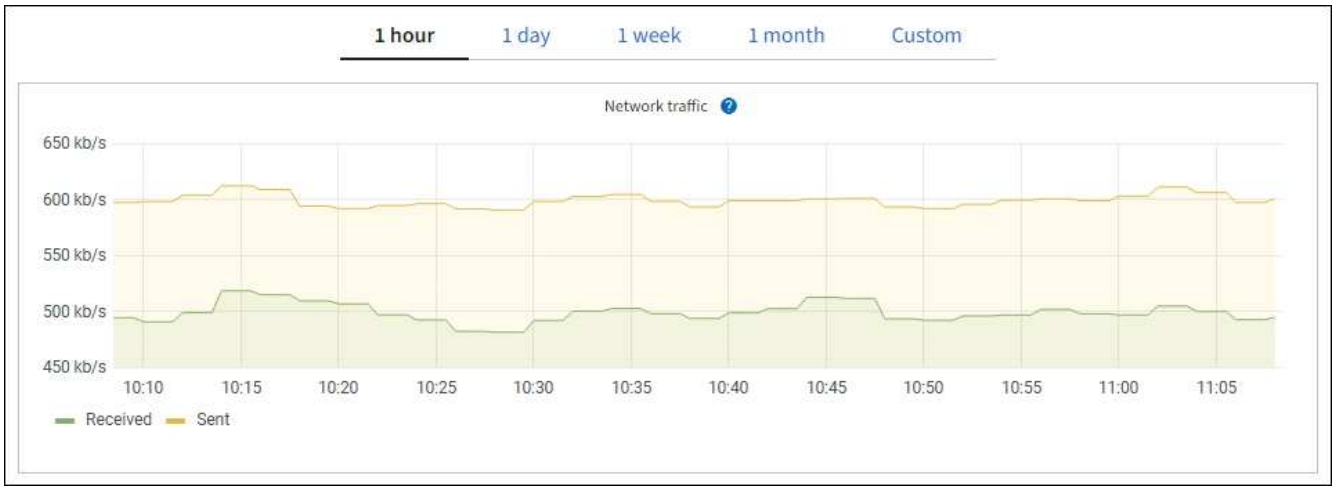
O que são métricas do Prometheus?

As métricas do Prometheus são medições de séries temporais. O serviço Prometheus nos nós administrativos coleta essas métricas dos serviços em todos os nós. As métricas são armazenadas em cada nó administrativo até que o espaço reservado para dados do Prometheus esteja cheio. Quando o `/var/local/mysql_ibdata/` quando o volume atinge a capacidade, as métricas mais antigas são excluídas primeiro.

Onde as métricas do Prometheus são usadas?

As métricas coletadas pelo Prometheus são usadas em vários lugares no Grid Manager:

- **Página Nós**: Os gráficos e tabelas nas guias disponíveis na página Nós usam a ferramenta de visualização Grafana para exibir as métricas de séries temporais coletadas pelo Prometheus. O Grafana exibe dados de séries temporais em formatos de gráfico e tabela, enquanto o Prometheus serve como fonte de dados de back-end.



- **Alertas**: Os alertas são acionados em níveis de gravidade específicos quando as condições da regra de alerta que usam métricas do Prometheus são avaliadas como verdadeiras.
- **API de gerenciamento de grade**: você pode usar métricas do Prometheus em regras de alerta personalizadas ou com ferramentas de automação externas para monitorar seu sistema StorageGRID . Uma lista completa de métricas do Prometheus está disponível na API de gerenciamento de grade. (Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API** > **métricas**.) Embora mais de mil métricas estejam disponíveis, apenas um número relativamente pequeno é necessário para monitorar as operações mais críticas do StorageGRID .

> Métricas que incluem *private* em seus nomes são destinadas apenas para uso interno e estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- A página **SUPORTE** > **Ferramentas** > **Diagnóstico** e a página **SUPORTE** > **Ferramentas** > **Métricas**: Essas páginas, que são destinadas principalmente ao uso do suporte técnico, fornecem diversas ferramentas e gráficos que usam os valores das métricas do Prometheus.

> Alguns recursos e itens de menu na página Métricas são intencionalmente não funcionais e estão sujeitos a alterações.

Lista das métricas mais comuns

A lista a seguir contém as métricas do Prometheus mais comumente usadas.

> Métricas que incluem *private* em seus nomes são apenas para uso interno e estão sujeitas a alterações sem aviso prévio entre as versões do StorageGRID .

alertmanager_notifications_failed_total
O número total de notificações de alerta com falha.

bytes disponíveis do sistema de arquivos do nó
A quantidade de espaço do sistema de arquivos disponível para usuários não root em bytes.

node_memory_MemAvailable_bytes
Campo de informações de memória MemAvailable_bytes.

portadora_de_rede_nó
Valor da transportadora de `/sys/class/net/`*`iface`* .

total_de_erros_de_recebimento_de_nó_rede
Estatística do dispositivo de rede `receive_errs` .

total_de_erros_de_transmissão_de_nó
Estatística do dispositivo de rede `transmit_errs` .

storagegrid_administrativamente_inativo
O nó não está conectado à rede por um motivo esperado. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado.

status_do_hardware_do_controlador_de_computação_do_dispositivo_de_grade_de_armazenamento
O status do hardware do controlador de computação em um dispositivo.

storagegrid_appliance_discos_com_falha
Para o controlador de armazenamento em um dispositivo, o número de unidades que não são ideais.

status do hardware do controlador de armazenamento do dispositivo de grade de armazenamento
O status geral do hardware do controlador de armazenamento em um dispositivo.

baldes_e_contêineres_de_conteúdo_da_grade_de_armazenamento
O número total de buckets S3 e contêineres Swift conhecidos por este nó de armazenamento.

objetos_de_conteúdo_da_grade_de_armazenamento
O número total de objetos de dados S3 e Swift conhecidos por este nó de armazenamento. A contagem é

válida somente para objetos de dados criados por aplicativos clientes que fazem interface com o sistema por meio do S3.

objetos_de_conteúdo_da_grade_de_armazenamento_perdidos

O número total de objetos que este serviço detecta como ausentes no sistema StorageGRID . Devem ser tomadas medidas para determinar a causa da perda e se a recuperação é possível.

"Solucionar problemas de dados de objetos perdidos e ausentes"

tentativas de entrada de sessões http da grade de armazenamento

O número total de sessões HTTP que foram tentadas em um nó de armazenamento.

storagegrid_http_sessions_incoming_atualmente_estabelecidas

O número de sessões HTTP que estão atualmente ativas (abertas) no nó de armazenamento.

storagegrid_http_sessions_incoming_failed

O número total de sessões HTTP que não foram concluídas com sucesso, seja devido a uma solicitação HTTP malformada ou a uma falha durante o processamento de uma operação.

storagegrid_http_sessions_incoming_sucesso

O número total de sessões HTTP que foram concluídas com sucesso.

storagegrid_ilm_aguardando_objetos_de_fundo

O número total de objetos neste nó aguardando avaliação do ILM da verificação.

storagegrid_ilm_aguardando_objetos_de_avaliação_do_cliente_por_segundo

A taxa atual na qual os objetos são avaliados em relação à política ILM neste nó.

storagegrid_ilm_aguardando_objetos_do_cliente

O número total de objetos neste nó aguardando avaliação do ILM de operações do cliente (por exemplo, ingestão).

storagegrid_ilm_aguardando_total_objetos

O número total de objetos aguardando avaliação do ILM.

storagegrid_ilm_scan_objetos_por_segundo

A taxa na qual os objetos pertencentes a este nó são verificados e enfileirados para ILM.

período_de_varredura_do_ilm_da_grade_de_armazenamento_minutos_estimados

Tempo estimado para concluir uma varredura ILM completa neste nó.

Observação: uma verificação completa não garante que o ILM foi aplicado a todos os objetos pertencentes a este nó.

tempo_de_expiração_do_certificado_do_endpoint_do_balanceador_de_carga_da_grade_de_armazenamento

O tempo de expiração do certificado do ponto de extremidade do balanceador de carga em segundos desde a época.

consultas_de_metadados_da_grade_de_armazenamento_latência_média_em_milissegundos

O tempo médio necessário para executar uma consulta no repositório de metadados por meio deste serviço.

bytes_recebidos_da_rede_de_grade_de_armazenamento

A quantidade total de dados recebidos desde a instalação.

bytes_transmitidos_da_rede_de_grade_de_armazenamento

A quantidade total de dados enviados desde a instalação.

porcentagem_de_utilização_da_cpu_do_nó_da_grade_de_armazenamento

A porcentagem de tempo de CPU disponível atualmente sendo usada por este serviço. Indica o quão ocupado o serviço está. A quantidade de tempo de CPU disponível depende do número de CPUs do servidor.

storagegrid_ntp_tempo_fonte_escolhido_deslocamento_em_milissegundos

Deslocamento sistemático de tempo fornecido por uma fonte de tempo escolhida. O deslocamento é introduzido quando o atraso para atingir uma fonte de tempo não é igual ao tempo necessário para que a fonte de tempo atinja o cliente NTP.

storagegrid_ntp_bloqueado

O nó não está bloqueado para um servidor NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

A quantidade total de dados ingeridos de clientes S3 para este nó de armazenamento desde a última redefinição do atributo.

storagegrid_s3_data_transfers_bytes_retrieved

A quantidade total de dados recuperados pelos clientes S3 deste nó de armazenamento desde a última redefinição do atributo.

storagegrid_s3_operations_failed

O número total de operações S3 com falha (códigos de status HTTP 4xx e 5xx), excluindo aquelas causadas por falha de autorização S3.

storagegrid_s3_operations_successful

O número total de operações S3 bem-sucedidas (código de status HTTP 2xx).

storagegrid_s3_operations_unauthorized

O número total de operações S3 com falha que são resultado de uma falha de autorização.

dias_de_expiração_do_certificado_do_servidor_de_grade_de_armazenamento_da_interface_de_gerenciamento_do_certificado

O número de dias antes do certificado da Interface de Gerenciamento expirar.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

O número de dias antes da expiração do certificado da API de armazenamento de objetos.

segundos_da_cpu_do_serviço_da_grade_de_armazenamento

A quantidade cumulativa de tempo que a CPU foi usada por este serviço desde a instalação.

bytes_de_uso_de_memória_do_serviço_de_grade_de_armazenamento

A quantidade de memória (RAM) atualmente em uso por este serviço. Este valor é idêntico ao exibido pelo utilitário Linux top como RES.

bytes_recebidos_da_rede_de_serviço_de_grade_de_armazenamento

A quantidade total de dados recebidos por este serviço desde a instalação.

bytes_transmitidos_pela_rede_de_serviço_de_grade_de_armazenamento

A quantidade total de dados enviados por este serviço.

reinicializações do serviço de storagegrid

O número total de vezes que o serviço foi reiniciado.

segundos_de_tempo_de_execução_do_serviço_de_grade_de_armazenamento

O tempo total em que o serviço está em execução desde a instalação.

segundos_de_tempo_de_atividade_do_serviço_da_grade_de_armazenamento

O tempo total em que o serviço ficou em execução desde que foi reiniciado pela última vez.

estado_de_armazenamento_atual_da_grade_de_armazenamento

O estado atual dos serviços de armazenamento. Os valores dos atributos são:

- 10 = Off-line
- 15 = Manutenção
- 20 = Somente leitura
- 30 = On-line

status_de_armazenamento_da_grade_de_armazenamento

O status atual dos serviços de armazenamento. Os valores dos atributos são:

- 0 = Sem erros
- 10 = Em transição
- 20 = Espaço livre insuficiente
- 30 = Volume(s) indisponíveis
- 40 = Erro

bytes_de_dados_de_utilização_de_armazenamento_da_grade_de_armazenamento

Uma estimativa do tamanho total de dados de objetos replicados e codificados para eliminação no Nó de Armazenamento.

utilização_de_metadados_de_armazenamento_da_grade_de_armazenamento_bytes_permitidos

O espaço total no volume 0 de cada nó de armazenamento permitido para metadados de objeto. Esse valor é sempre menor que o espaço real reservado para metadados em um nó, porque uma parte do espaço reservado é necessária para operações essenciais do banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço permitido para metadados de objetos controla a capacidade geral do objeto.

bytes_de_metadados_de_utilização_de_armazenamento_da_grade_de_armazenamento

A quantidade de metadados do objeto no volume de armazenamento 0, em bytes.

utilização_de_armazenamento_da_grade_de_armazenamento_total_de_bytes_de_espaço

A quantidade total de espaço de armazenamento alocado para todos os armazenamentos de objetos.

utilização_de_armazenamento_da_grade_de_armazenamento_bytes_de_espaço_utilizável

A quantidade total de espaço de armazenamento de objetos restante. Calculado somando a quantidade de espaço disponível para todos os armazenamentos de objetos no Nó de Armazenamento.

storagegrid_swift_data_transfers_bytes_ingestados

A quantidade total de dados ingeridos de clientes Swift para este nó de armazenamento desde a última redefinição do atributo.

storagegrid_swift_data_transfers_bytes_recuperados

A quantidade total de dados recuperados pelos clientes Swift deste nó de armazenamento desde a última redefinição do atributo.

falha nas operações rápidas da grade de armazenamento

O número total de operações Swift com falha (códigos de status HTTP 4xx e 5xx), excluindo aquelas causadas por falha de autorização Swift.

storagegrid_swift_operações_bem-sucedidas

O número total de operações Swift bem-sucedidas (código de status HTTP 2xx).

storagegrid_swift_operações_não autorizadas

O número total de operações Swift com falha que são resultado de uma falha de autorização (códigos de status HTTP 401, 403, 405).

bytes de dados de uso do locatário da grade de armazenamento

O tamanho lógico de todos os objetos para o locatário.

contagem_de_objetos_de_uso_do_locatário_da_grade_de_armazenamento

O número de objetos para o inquilino.

cota_bytes_de_uso_do_locatário_da_grade_de_armazenamento

A quantidade máxima de espaço lógico disponível para os objetos do locatário. Se uma métrica de cota não for fornecida, uma quantidade ilimitada de espaço estará disponível.

Obtenha uma lista de todas as métricas

Para obter a lista completa de métricas, use a API de gerenciamento de grade.

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Localize as operações **métricas**.
3. Executar o `GET /grid/metric-names` operação.
4. Baixe os resultados.

Referência de arquivos de log

Referência de arquivos de log

O StorageGRID fornece logs que são usados para capturar eventos, mensagens de diagnóstico e condições de erro. Você pode ser solicitado a coletar arquivos de log e encaminhá-los ao suporte técnico para ajudar na solução de problemas.

Os logs são categorizados da seguinte forma:

- "Registros do software StorageGRID"
- "Registros de implantação e manutenção"
- "Sobre o bycast.log"

> Os detalhes fornecidos para cada tipo de log são apenas para referência. Os logs são destinados à solução de problemas avançada pelo suporte técnico. Técnicas avançadas que envolvem a reconstrução do histórico de problemas usando os logs de auditoria e os arquivos de log do aplicativo estão além do escopo destas instruções.

Acessar os logs

Para acessar os logs, você pode"coletar arquivos de log e dados do sistema" de um ou mais nós como um único arquivo de log. Ou, se o nó de administração principal não estiver disponível ou não conseguir acessar um nó específico, você poderá acessar arquivos de log individuais para cada nó de grade da seguinte maneira:

1. Digite o seguinte comando: `ssh admin@grid_node_IP`
2. Digite a senha listada no `Passwords.txt` arquivo.
3. Digite o seguinte comando para alternar para root: `su -`
4. Digite a senha listada no `Passwords.txt` arquivo.

Exportar logs para o servidor syslog

Exportar os logs para o servidor syslog fornece estes recursos:

- Receba uma lista de todas as solicitações do Grid Manager e do Tenant Manager, além das solicitações do S3 e do Swift.
- Melhor visibilidade das solicitações do S3 que retornam erros, sem o impacto no desempenho causado pelos métodos de registro de auditoria.
- Acesso a solicitações de camada HTTP e códigos de erro fáceis de analisar.
- Melhor visibilidade das solicitações que foram bloqueadas pelos classificadores de tráfego no balanceador de carga.

Para exportar os logs, consulte"Configurar mensagens de auditoria e destinos de log" .

Categorias de arquivos de log

O arquivo de log do StorageGRID contém os logs descritos para cada categoria e arquivos adicionais que contêm métricas e saída de comando de depuração.

Localização do arquivo	Descrição
auditoria	Mensagens de auditoria geradas durante a operação normal do sistema.
base-os-logs	Informações básicas do sistema operacional, incluindo versões de imagem do StorageGRID .

Localização do arquivo	Descrição
pacotes	Informações de configuração global (pacotes).
Cassandra	Informações do banco de dados Cassandra e logs de reparo do Reaper.
CE	Informações do VCS sobre o nó atual e informações do grupo EC por ID de perfil.
grade	Registros gerais da grade, incluindo depuração(`bycast.log`) e `servermanager` registros.
grade.json	Arquivo de configuração de grade compartilhado entre todos os nós. Adicionalmente, `node.json` é específico para o nó atual.
hagrupos	Métricas e logs de grupos de alta disponibilidade.
instalar	`Gdu-server`e instalar logs.
Lambda-árbitro	Logs relacionados à solicitação de proxy do S3 Select.
lenhador.log	Mensagens de depuração relacionadas à coleta de logs.
Métricas	Logs de serviço para Grafana, Jaeger, exportador de nós e Prometheus.
miscd	Acessos e logs de erros diversos.
MySQL	A configuração do banco de dados mariaDB e logs relacionados.
líquido	Logs gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos de configuração e logs do balanceador de carga e da federação de grade. Inclui também registros de tráfego do Grid Manager e do Tenant Manager.

Localização do arquivo	Descrição
nginx-gw	• `access.log`: Mensagens de log de solicitações do Grid Manager e do Tenant Manager. ◦ Essas mensagens são prefixadas com `mgmt:` quando exportado usando syslog. ◦ O formato dessas mensagens de log é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Solicitações de replicação entre grades de entrada. ◦ Essas mensagens são prefixadas com `cgr:` quando exportado usando syslog. ◦ O formato dessas mensagens de log é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: Solicitações S3 e Swift para endpoints do balanceador de carga. ◦ Essas mensagens são prefixadas com `endpoint:` quando exportado usando syslog. ◦ O formato dessas mensagens de log é `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Relacionado ao novo alerta de verificação de DNS.
ntp	Arquivo de configuração e logs do NTP.
Objetos órfãos	Registros referentes a objetos órfãos.
sistema operacional	Arquivo de estado de nó e grade, incluindo serviços `pid` .
outro	Arquivos de log em `/var/local/log` que não são coletados em outras pastas.
desempenho	Informações de desempenho para CPU, rede e E/S de disco.
prometheus-data	Métricas atuais do Prometheus, se a coleção de logs incluir dados do Prometheus.
provisionamento	Logs relacionados ao processo de provisionamento da rede.
jangada	Logs do cluster Raft usados em serviços de plataforma.

Localização do arquivo	Descrição
ssh	Logs relacionados à configuração e serviço SSH.
snmp	Configuração do agente SNMP usada para enviar notificações SNMP.
soquetes-dados	Dados de soquetes para depuração de rede.
comandos-do-sistema.txt	Saída dos comandos do contêiner StorageGRID . Contém informações do sistema, como rede e uso de disco.
pacote de recuperação de sincronização	Relacionado à manutenção da consistência do Pacote de Recuperação mais recente em todos os Nós de Administração e Nós de Armazenamento que hospedam o serviço ADC.

Registros do software StorageGRID

Você pode usar os logs do StorageGRID para solucionar problemas.

Se você deseja enviar seus logs para um servidor syslog externo ou alterar o destino das informações de auditoria, como `bycast.log` e `nms.log` , ver"Configurar mensagens de auditoria e destinos de log" .

Logs do StorageGRID geral

Nome do arquivo	Notas	Encontrado em
/var/local/log/bycast.log	O arquivo principal de solução de problemas do StorageGRID . Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**. Em seguida, selecione ***Site*** > ***Nó*** > **SSM** > **Eventos**.	Todos os nós
/var/local/log/bycast-err.log	Contém um subconjunto de `bycast.log` (mensagens com gravidade ERRO e CRÍTICO). Mensagens CRÍTICAS também são exibidas no sistema. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**. Em seguida, selecione ***Site*** > ***Nó*** > **SSM** > **Eventos**.	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/núcleo/	Contém todos os arquivos de despejo de memória criados caso o programa seja encerrado de forma anormal. As causas possíveis incluem falhas de asserção, violações ou tempos limite de thread. **Nota**: O arquivo `/var/local/core/kexec_cmd` geralmente existe em nós de dispositivos e não indica um erro.	Todos os nós

Registros relacionados à cifra

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssh-config-generation.log	Contém logs relacionados à geração de configurações SSH e ao recarregamento de serviços SSH.	Todos os nós
/var/local/log/nginx/config-generation.log	Contém logs relacionados à geração de configurações nginx e ao recarregamento de serviços nginx.	Todos os nós
/var/local/log/nginx-gw/config-generation.log	Contém logs relacionados à geração de configurações do nginx-gw (e ao recarregamento de serviços do nginx-gw).	Nós de administração e gateway
/var/local/log/atualizar-configurações-de-cifra.log	Contém logs relacionados à configuração de políticas TLS e SSH.	Todos os nós

Registros de federação de grade

Nome do arquivo	Notas	Encontrado em
/var/local/log/update_grid_federation_config.log	Contém logs relacionados à geração de configurações nginx e nginx-gw para conexões de federação de grade.	Todos os nós

Registros NMS

Nome do arquivo	Notas	Encontrado em
/var/local/log/nms.log	• Captura notificações do Grid Manager e do Tenant Manager. • Captura eventos relacionados à operação do serviço NMS. Por exemplo, notificações por e-mail e alterações de configuração. • Contém atualizações de pacotes XML resultantes de alterações de configuração feitas no sistema. • Contém mensagens de erro relacionadas à redução de amostragem de atributos feita uma vez por dia. • Contém mensagens de erro do servidor web Java, por exemplo, erros de geração de página e erros HTTP Status 500.	Nós de administração
/var/local/log/nms.errlog	Contém mensagens de erro relacionadas a atualizações do banco de dados MySQL. Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de administração
/var/local/log/nms.requestlog	Contém informações sobre conexões de saída da API de gerenciamento para serviços internos do StorageGRID .	Nós de administração

Logs do Gerenciador de Servidores

Nome do arquivo	Notas	Encontrado em
/var/local/log/servermanager.log	Arquivo de log do aplicativo Gerenciador do Servidor em execução no servidor.	Todos os nós
/var/local/log/GridstatBackend.errlog	Arquivo de log para o aplicativo de backend da GUI do Gerenciador do Servidor.	Todos os nós
/var/local/log/gridstat.errlog	Arquivo de log para a GUI do Gerenciador do Servidor.	Todos os nós

Registros de serviços do StorageGRID

Nome do arquivo	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/adc.errlog	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de armazenamento executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/cassandra/system.log	Informações para o armazenamento de metadados (banco de dados Cassandra) que podem ser usadas se ocorrerem problemas ao adicionar novos nós de armazenamento ou se a tarefa de reparo do nodetool parar.	Nós de armazenamento
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que realiza reparos dos dados no banco de dados Cassandra.	Nós de armazenamento
/var/local/log/cassandra-reaper.errlog	Informações de erro para o serviço Cassandra Reaper.	Nós de armazenamento
/var/local/log/chunk.errlog		Nós de armazenamento
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Este arquivo de log pode estar presente em sistemas que foram atualizados de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de armazenamento
/var/local/log/dds.errlog		Nós de armazenamento
/var/local/log/dmv.errlog		Nós de armazenamento
/var/local/log/dynip*	Contém logs relacionados ao serviço dynip, que monitora a grade em busca de alterações dinâmicas de IP e atualiza a configuração local.	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/log/grafana.log	O log associado ao serviço Grafana, que é usado para visualização de métricas no Grid Manager.	Nós de administração
/var/local/log/hagroups.log	O log associado aos grupos de alta disponibilidade.	Nós de administração e nós de gateway
/var/local/log/hagroups_events.log	Rastreia mudanças de estado, como transição de BACKUP para MASTER ou FAULT.	Nós de administração e nós de gateway
/var/local/log/idnt.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/jaeger.log	O log associado ao serviço jaeger, que é usado para coleta de rastreamento.	Todos os nós
/var/local/log/kstn.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/lambda*	Contém logs para o serviço S3 Select.	Nós de administração e gateway Somente certos nós de administração e gateway contêm esse log. Veja o"Requisitos e limitações do S3 Select para nós de administração e gateway" .
/var/local/log/ldr.errlog		Nós de armazenamento
/var/local/log/miscd/*.log	Contém logs para o serviço MISCd (Information Service Control Daemon), que fornece uma interface para consultar e gerenciar serviços em outros nós e para gerenciar configurações ambientais no nó, como consultar o estado de serviços em execução em outros nós.	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/log/nginx/*.log	Contém logs para o serviço nginx, que atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e Dynip) para poder se comunicar com serviços em outros nós por meio de APIs HTTPS.	Todos os nós
/var/local/log/nginx-gw/*.log	Contém logs gerais relacionados ao serviço nginx-gw, incluindo logs de erros e logs para portas de administração restritas em nós de administração.	Nós de administração e nós de gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contém logs de acesso relacionados ao tráfego de replicação entre redes.	Nós de administração, nós de gateway ou ambos, com base na configuração de federação da grade. Encontrado somente na grade de destino para replicação entre grades.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contém logs de acesso para o serviço Load Balancer, que fornece balanceamento de carga do tráfego S3 de clientes para nós de armazenamento.	Nós de administração e nós de gateway
/var/local/log/persistence*	Contém logs para o serviço Persistência, que gerencia arquivos no disco raiz que precisam persistir após uma reinicialização.	Todos os nós
/var/local/log/prometheus.log	Para todos os nós, contém o log de serviço do exportador de nós e o log de serviço de métricas do ade-exporter. Para nós de administração, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós
/var/local/log/raft.log	Contém a saída da biblioteca usada pelo serviço RSM para o protocolo Raft.	Nós de armazenamento com serviço RSM
/var/local/log/rms.errlog	Contém logs para o serviço Replicated State Machine Service (RSM), que é usado para serviços da plataforma S3.	Nós de armazenamento com serviço RSM

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssm.errlog		Todos os nós
/var/local/log/atualização-s3vs-domains.log	Contém logs relacionados ao processamento de atualizações para a configuração de nomes de domínio hospedados virtuais do S3. Consulte as instruções para implementar aplicativos cliente do S3.	Nós de administração e gateway
/var/local/log/atualização-snmp-firewall.*	Contém logs relacionados às portas do firewall gerenciadas para SNMP.	Todos os nós
/var/local/log/atualização-sysl.log	Contém logs relacionados às alterações feitas na configuração do syslog do sistema.	Todos os nós
/var/local/log/atualizar-classes-de-trafego.log	Contém logs relacionados a alterações na configuração dos classificadores de tráfego.	Nós de administração e gateway
/var/local/log/update-utcn.log	Contém logs relacionados ao modo de rede de cliente não confiável neste nó.	Todos os nós

Informações relacionadas

- "Sobre o bycast.log"
- "Usar API REST do S3"

Registros de implantação e manutenção

Você pode usar os logs de implantação e manutenção para solucionar problemas.

Nome do arquivo	Notas	Encontrado em
/var/local/log/install.log	Criado durante a instalação do software. Contém um registro dos eventos de instalação.	Todos os nós
/var/local/log/expansion-progress.log	Criado durante as operações de expansão. Contém um registro dos eventos de expansão.	Nós de armazenamento
/var/local/log/pa-move.log	Criado durante a execução do `pa-move.sh` roteiro.	Nó de administração primário
/var/local/log/pa-move-new_pa.log	Criado durante a execução do `pa-move.sh` roteiro.	Nó de administração primário

Nome do arquivo	Notas	Encontrado em
/var/local/log/pa-move-old_pa.log	Criado durante a execução do `pa-move.sh` roteiro.	Nó de administração primário
/var/local/log/gdu-server.log	Criado pelo serviço GDU. Contém eventos relacionados aos procedimentos de provisionamento e manutenção gerenciados pelo nó de administração principal.	Nó de administração primário
/var/local/log/send_admin_hw.log	Criado durante a instalação. Contém informações de depuração relacionadas às comunicações de um nó com o nó de administração principal.	Todos os nós
/var/local/log/upgrade.log	Criado durante a atualização do software. Contém um registro dos eventos de atualização de software.	Todos os nós

Sobre o bycast.log

O arquivo `/var/local/log/bycast.log` é o arquivo principal de solução de problemas do software StorageGRID . Há um `bycast.log` arquivo para cada nó da grade. O arquivo contém mensagens específicas para aquele nó da grade.

O arquivo `/var/local/log/bycast-err.log` é um subconjunto de `bycast.log` . Ele contém mensagens de gravidade ERRO e CRÍTICO.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver "Configurar mensagens de auditoria e destinos de log" .

Rotação de arquivos para bycast.log

Quando o `bycast.log` o arquivo atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado.

O arquivo salvo é renomeado `bycast.log.1` , e o novo arquivo é nomeado `bycast.log` . Quando o novo `bycast.log` atinge 1 GB, `bycast.log.1` é renomeado e compactado para se tornar `bycast.log.2.gz` , e `bycast.log` é renomeado `bycast.log.1` .

O limite de rotação para `bycast.log` são 21 arquivos. Quando a 22ª versão do `bycast.log` arquivo é criado, o arquivo mais antigo é excluído.

O limite de rotação para `bycast-err.log` são sete arquivos.

> ⓘ Se um arquivo de log foi compactado, você não deve descompactá-lo no mesmo local em que foi gravado. Descompactar o arquivo no mesmo local pode interferir nos scripts de rotação de log.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver "Configurar mensagens de auditoria e destinos de log" .

Informações relacionadas

"Coletar arquivos de log e dados do sistema"

Mensagens em bycast.log

Mensagens em `bycast.log` são escritos pelo ADE (Ambiente Distribuído Assíncrono). ADE é o ambiente de execução usado pelos serviços de cada nó da grade.

Exemplo de mensagem ADE:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

As mensagens ADE contêm as seguintes informações:

Segmento de mensagem	Valor no exemplo
ID do nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador de mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.uuuuuu)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação de integridade do volume 3 falhou com o motivo 'TOUT'

Gravidade das mensagens em bycast.log

As mensagens em `bycast.log` são atribuídos níveis de gravidade.

Por exemplo:

- **AVISO** — Ocorreu um evento que deveria ser registrado. A maioria das mensagens de log estão neste nível.
- **AVISO** — Ocorreu uma condição inesperada.
- **ERRO** — Ocorreu um erro grave que afetará as operações.
- **CRÍTICO** — Ocorreu uma condição anormal que interrompeu as operações normais. Você deve tratar a condição subjacente imediatamente.

Códigos de erro em `bycast.log`

A maioria das mensagens de erro em `bycast.log` contêm códigos de erro.

A tabela a seguir lista códigos não numéricos comuns em `bycast.log` . O significado exato de um código não numérico depende do contexto em que ele é relatado.

Código de erro	Significado
SUCS	Nenhum erro
GERR	Desconhecido
CANC	Cancelado
ABRT	Abortado
TOTALMENTE	Tempo esgotado
INVL	Inválido
NFND	Não encontrado
VERS	Versão
CONF	Configuração
FALHAR	Fracassado
ICPL	Incompleto
FEITO	Feito
SUNV	Serviço não disponível

A tabela a seguir lista os códigos de erro numéricos em `bycast.log` .

Número do erro	Código de erro	Significado
001	EPERM	Operação não permitida
002	ENOENTE	Não existe tal arquivo ou diretório
003	ESRCH	Não existe tal processo
004	EINTR	Chamada de sistema interrompida

Número do erro	Código de erro	Significado
005	EIO	Erro de E/S
006	ENXIO	Nenhum dispositivo ou endereço desse tipo
007	E2BIG	Lista de argumentos muito longa
008	ENOEXEC	Erro de formato Exec
009	EBADF	Número de arquivo inválido
010	CRIANÇA	Nenhum processo filho
011	NOVAMENTE	Tente novamente
012	ENOMEM	Sem memória
013	EACCES	Permissão negada
014	FALHA	Endereço incorreto
015	ENOTBLK	Dispositivo de bloqueio necessário
016	EBUSY	Dispositivo ou recurso ocupado
017	EEXIST	O arquivo existe
018	EXDEV	Link entre dispositivos
019	ENODEV	Nenhum dispositivo desse tipo
020	ENOTDIR	Não é um diretório
021	EISDIR	É um diretório
022	EINVAL	Argumento inválido
023	ENFILE	Estouro de tabela de arquivos
024	EMFILE	Muitos arquivos abertos
025	NÃO É NADA	Não é uma máquina de escrever
026	ETXTBSY	Arquivo de texto ocupado

Número do erro	Código de erro	Significado
027	EFBIG	Arquivo muito grande
028	ENOSPC	Não há espaço disponível no dispositivo
029	ESPIAR	Busca ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Muitos links
032	EPIPE	Cano quebrado
033	EDOM	Argumento matemático fora do domínio da função
034	ERRANGE	Resultado matemático não representável
035	EDEADLK	Ocorreria um impasse de recursos
036	ENAMETOOLONG	Nome do arquivo muito longo
037	ENOLCK	Nenhum bloqueio de registro disponível
038	ENOSYS	Função não implementada
039	ENOTEMPTY	Diretório não vazio
040	ELOOP	Muitos links simbólicos encontrados
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido
044	ECHRNG	Número do canal fora do intervalo
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Redefinição de nível 3
048	ELNRNG	Número do link fora do intervalo

Número do erro	Código de erro	Significado
049	EUNATCHE	Driver de protocolo não anexado
050	ENOCSI	Nenhuma estrutura CSI disponível
051	EL2HLT	Nível 2 interrompido
052	EBADE	Troca inválida
053	EBADR	Descritor de solicitação inválido
054	EXFULL	Troca completa
055	ENOANO	Sem ânodo
056	EBADRQC	Código de solicitação inválido
057	EBADSLT	Slot inválido
058		
059	EBFONT	Formato de arquivo de fonte incorreto
060	ENOSTR	O dispositivo não é um fluxo
061	ENODADOS	Nenhum dado disponível
062	ETIME	Temporizador expirado
063	ENOSR	Recursos fora dos fluxos
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado
066	REMOTO	O objeto é remoto
067	ENOLINK	O link foi rompido
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação no envio

Número do erro	Código de erro	Significado
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de multi-hop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	EOVERFLOW	Valor muito grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em mau estado
078	EREMCHG	Endereço remoto alterado
079	ELIBACC	Não é possível acessar uma biblioteca compartilhada necessária
080	ELIBBAD	Acessando uma biblioteca compartilhada corrompida
081	ELIBSCN	
082	ELIBMAX	Tentando vincular muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada de sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro de canal de fluxos
087	USUÁRIOS	Muitos usuários
088	ENOTSOCK	Operação de soquete em não soquete
089	EDESTADDRREQ	Endereço de destino obrigatório
090	TAMANHO EMSGS	Mensagem muito longa

Número do erro	Código de erro	Significado
091	EPROTÓTIPO	Protocolo tipo errado para soquete
092	ENOPROTOOPT	Protocolo não disponível
093	EPROTONOSUPPORT	Protocolo não suportado
094	SUPORTE ESOCKTNOS	Tipo de soquete não suportado
095	EOPNOTSUPP	Operação não suportada no ponto de extremidade de transporte
096	EPFNOSUPPORT	Família de protocolo não suportada
097	APOIO EAFNOS	Família de endereços não suportada pelo protocolo
098	USO DE DRINCO PRINCIPAL	Endereço já em uso
099	EDDRNOTAVAIL	Não é possível atribuir o endereço solicitado
100	ENETDOWN	A rede está inativa
101	ENETUNREACH	A rede está inacessível
102	ENETRESET	A rede perdeu a conexão devido à reinicialização
103	ECONNABORTED	O software causou o encerramento da conexão
104	REINICIALIZAÇÃO ECONÔMICA	Conexão redefinida pelo peer
105	ENOBUFS	Não há espaço de buffer disponível
106	EISCONN	O ponto final de transporte já está conectado
107	ENOTCONN	O ponto final de transporte não está conectado
108	DESLIGAMENTO	Não é possível enviar após o desligamento do ponto de extremidade de transporte
109	ETOOMANYREFS	Muitas referências: não é possível unir
110	ETIMEDOUT	Tempo de conexão esgotado
111	ECONOMIZADO RECUSADO	Ligação recusada

Número do erro	Código de erro	Significado
112	EHOSTDOWN	O host está inativo
113	EHOSTUNREACH	Nenhuma rota para o host
114	JÁ	Operação já em andamento
115	EINPROGRESS	Operação em andamento
116		
117	EUCLEAN	Estrutura precisa de limpeza
118	ENOTNAM	Não é um arquivo do tipo nomeado XENIX
119	DISPONIBILIZAR	Nenhum semáforo XENIX disponível
120	EISNAM	É um arquivo de tipo nomeado
121	EREMOTEIO	Erro de E/S remota
122	EDQUOT	Cota excedida
123	ENOMEDIUM	Nenhum meio encontrado
124	TIPO MÉDIO	Tipo de mídia errado
125	EXCANCELADO	Operação cancelada
126	ENOKEY	Chave necessária não disponível
127	EKEY EXPIRADA	A chave expirou
128	EKEY REVOGADA	A chave foi revogada
129	EKEYREJEITADO	A chave foi rejeitada pelo serviço
130	PROPRIETÁRIO MORTO	Para mutexes robustos: O proprietário faleceu
131	ENOTRECOVERABLE	Para mutexes robustos: Estado não recuperável

Configurar destinos de mensagens e logs de auditoria

Considerações para usar um servidor syslog externo

Um servidor syslog externo é um servidor fora do StorageGRID que você pode usar para coletar informações de auditoria do sistema em um único local. Usar um servidor syslog externo permite reduzir o tráfego de rede em seus nós de administração e gerenciar as informações com mais eficiência. Para StorageGRID, o formato do pacote de mensagens syslog de saída é compatível com RFC 3164.

Os tipos de informações de auditoria que você pode enviar ao servidor syslog externo incluem:

- Registros de auditoria contendo as mensagens de auditoria geradas durante a operação normal do sistema
- Eventos relacionados à segurança, como logins e escalonamentos para root
- Logs de aplicativos que podem ser solicitados caso seja necessário abrir um caso de suporte para solucionar um problema que você encontrou

Quando usar um servidor syslog externo

Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. O envio de informações de auditoria para um servidor syslog externo permite que você:

- Colete e gerencie informações de auditoria, como mensagens de auditoria, logs de aplicativos e eventos de segurança com mais eficiência.
- Reduza o tráfego de rede em seus nós de administração porque as informações de auditoria são transferidas diretamente dos vários nós de armazenamento para o servidor syslog externo, sem precisar passar por um nó de administração.

> Quando os logs são enviados para um servidor syslog externo, logs únicos maiores que 8.192 bytes são truncados no final da mensagem para estar em conformidade com as limitações comuns em implementações de servidores syslog externos.

> Para maximizar as opções de recuperação completa de dados em caso de falha do servidor syslog externo, até 20 GB de logs locais de registros de auditoria(`localaudit.log`) são mantidos em cada nó.

Como configurar um servidor syslog externo

Para aprender como configurar um servidor syslog externo, consulte"Configurar mensagens de auditoria e servidor syslog externo" .

Se você planeja configurar o uso do protocolo TLS ou RELP/TLS, você deve ter os seguintes certificados:

- **Certificados de CA do servidor**: Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo na codificação PEM. Se omitido, o certificado Grid CA padrão será usado.
- **Certificado do cliente**: O certificado do cliente para autenticação no servidor syslog externo na codificação PEM.
- **Chave privada do cliente**: Chave privada para o certificado do cliente na codificação PEM.

Se você usar um certificado de cliente, também deverá usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, também deverá fornecer a senha. Não há benefício significativo de segurança no uso de uma chave privada criptografada porque a chave e a senha devem ser armazenadas; usar uma chave privada não criptografada, se disponível, é recomendado para simplificar.

Como estimar o tamanho do servidor syslog externo

Normalmente, sua grade é dimensionada para atingir uma taxa de transferência necessária, definida em termos de operações S3 por segundo ou bytes por segundo. Por exemplo, você pode ter um requisito para que sua grade manipule 1.000 operações S3 por segundo, ou 2.000 MB por segundo, de ingestões e recuperações de objetos. Você deve dimensionar seu servidor syslog externo de acordo com os requisitos de dados da sua grade.

Esta seção fornece algumas fórmulas heurísticas que ajudam você a estimar a taxa e o tamanho médio de mensagens de log de vários tipos que seu servidor syslog externo precisa ser capaz de manipular, expressos em termos das características de desempenho conhecidas ou desejadas da grade (operações S3 por segundo).

Use operações S3 por segundo em fórmulas de estimativa

Se sua grade foi dimensionada para uma taxa de transferência expressa em bytes por segundo, você deve converter esse dimensionamento em operações S3 por segundo para usar as fórmulas de estimativa. Para converter a taxa de transferência da grade, você deve primeiro determinar o tamanho médio do objeto, o que pode ser feito usando as informações em logs de auditoria e métricas existentes (se houver) ou usando seu conhecimento dos aplicativos que usarão o StorageGRID. Por exemplo, se sua grade foi dimensionada para atingir uma taxa de transferência de 2.000 MB/segundo, e seu tamanho médio de objeto é de 2 MB, então sua grade foi dimensionada para poder lidar com 1.000 operações S3 por segundo (2.000 MB / 2 MB).

As fórmulas para dimensionamento do servidor syslog externo nas seções a seguir fornecem estimativas de casos comuns (em vez de estimativas de pior caso). Dependendo da sua configuração e carga de trabalho, você poderá ver uma taxa maior ou menor de mensagens do syslog ou um volume de dados do syslog do que o previsto pelas fórmulas. As fórmulas devem ser usadas apenas como diretrizes.

Fórmulas de estimativa para registros de auditoria

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 por segundo que sua grade deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, supondo que você deixe os Níveis de Auditoria definidos com os valores padrão (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 2.000 mensagens syslog por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de 1,6 MB por segundo.

Se você souber mais sobre sua carga de trabalho, estimativas mais precisas serão possíveis. Para logs de

auditoria, as variáveis adicionais mais importantes são a porcentagem de operações S3 que são PUTs (vs. GETS) e o tamanho médio, em bytes, dos seguintes campos S3 (as abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Vamos usar P para representar a porcentagem de operações S3 que são PUTs, onde 0 ≤ P ≤ 1 (portanto, para uma carga de trabalho de 100% PUT, P = 1, e para uma carga de trabalho de 100% GET, P = 0).

Vamos usar K para representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então o valor de K é 90 (13+13+28+36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, supondo que você deixe os Níveis de Auditoria definidos como padrões (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.500 mensagens syslog por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de aproximadamente 1 MB por segundo.

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para logs de auditoria pressupõem o uso de configurações de nível de auditoria padrão (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro). Fórmulas detalhadas para estimar a taxa e o tamanho médio de mensagens de auditoria para configurações de nível de auditoria não padrão não estão disponíveis. No entanto, a tabela a seguir pode ser usada para fazer uma estimativa aproximada da taxa; você pode usar a fórmula de tamanho médio fornecida para logs de auditoria, mas esteja ciente de que isso provavelmente resultará em uma superestimativa porque as

mensagens de auditoria "extras" são, em média, menores que as mensagens de auditoria padrão.

Doença	Fórmula
Replicação: níveis de auditoria todos definidos como Depuração ou Normal	Taxa de log de auditoria = 8 x taxa de operações S3
Codificação de eliminação: níveis de auditoria todos definidos como Depuração ou Normal	Use a mesma fórmula das configurações padrão

Fórmulas de estimativa para eventos de segurança

Eventos de segurança não estão correlacionados com operações do S3 e normalmente produzem um volume insignificante de logs e dados. Por essas razões, nenhuma fórmula de estimativa é fornecida.

Fórmulas de estimativa para logs de aplicação

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 por segundo que sua grade deve suportar, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo precisará manipular usando as seguintes fórmulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Assim, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 3.300 logs de aplicativos por segundo e ser capaz de receber (e armazenar) dados de log de aplicativos a uma taxa de cerca de 1,2 MB por segundo.

Se você souber mais sobre sua carga de trabalho, estimativas mais precisas serão possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. codificação de eliminação), a porcentagem de operações S3 que são PUTs (vs. GETs/outros) e o tamanho médio, em bytes, dos seguintes campos S3 (as abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Exemplos de estimativas de dimensionamento

Esta seção explica casos de exemplo de como usar as fórmulas de estimativa para grades com os seguintes métodos de proteção de dados:

- Replicação
- Codificação de apagamento

Se você usar replicação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde 0 ≤ P ≤ 1 (portanto, para uma carga de trabalho de 100% PUT, P = 1, e para uma carga de trabalho de 100% GET, P = 0).

Deixe K representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13+13+28+36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando as seguintes fórmulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Assim, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.800 logs de aplicativos por segundo e receberá (e normalmente armazenará) dados de aplicativos a uma taxa de 0,5 MB por segundo.

Se você usar codificação de eliminação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde 0 ≤ P ≤ 1 (portanto, para uma carga de trabalho de 100% PUT, P = 1, e para uma carga de trabalho de 100% GET, P = 0).

Deixe K representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13+13+28+36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando as seguintes fórmulas.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Portanto, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 2.250 logs de aplicativos por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar mensagens de auditoria e servidor syslog externo

Você pode configurar uma série de configurações relacionadas às mensagens de auditoria. Você pode ajustar o número de mensagens de auditoria registradas; definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente; configurar um servidor syslog externo; e especificar para onde os logs de auditoria, logs de eventos de segurança e logs de software StorageGRID são enviados.

Mensagens e logs de auditoria registram atividades do sistema e eventos de segurança e são ferramentas essenciais para monitoramento e solução de problemas. Todos os nós do StorageGRID geram mensagens de auditoria e logs para rastrear atividades e eventos do sistema.

Opcionalmente, você pode configurar um servidor syslog externo para salvar informações de auditoria remotamente. Usar um servidor externo minimiza o impacto no desempenho do registro de mensagens de auditoria sem reduzir a integridade dos dados de auditoria. Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. Ver"Configurar mensagens de auditoria e servidor syslog externo" para mais detalhes.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .
- Se você planeja configurar um servidor syslog externo, você revisou o"considerações para usar um servidor syslog externo" e garantiu que o servidor tenha capacidade suficiente para receber e armazenar os arquivos de log.
- Se você planeja configurar um servidor syslog externo usando o protocolo TLS ou RELP/TLS, você tem a CA do servidor e os certificados de cliente necessários e a chave privada do cliente.

Alterar níveis de mensagens de auditoria

Você pode definir um nível de auditoria diferente para cada uma das seguintes categorias de mensagens no log de auditoria:

Categoria de auditoria	Configuração padrão	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"

Categoria de auditoria	Configuração padrão	Mais informações
Armazenar	Erro	"Mensagens de auditoria de armazenamento de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gestão"
O cliente lê	Normal	"O cliente leu mensagens de auditoria"
O cliente escreve	Normal	"O cliente escreve mensagens de auditoria"
ILM	Normal	"Mensagens de auditoria do ILM"
Replicação entre grades	Erro	"CGRR: Solicitação de replicação entre redes"

Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10.3 ou posterior. Se você usou inicialmente uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como Normal.

Durante as atualizações, as configurações de nível de auditoria não entrarão em vigor imediatamente.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**.
2. Para cada categoria de mensagem de auditoria, selecione um nível de auditoria na lista suspensa:

Nível de auditoria	Descrição
Desligado	Nenhuma mensagem de auditoria da categoria é registrada.
Erro	Somente mensagens de erro são registradas — mensagens de auditoria para as quais o código de resultado não foi "bem-sucedido" (SUCS).
Normal	Mensagens transacionais padrão são registradas — as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível se comporta da mesma forma que o nível de auditoria Normal.

As mensagens incluídas para qualquer nível específico incluem aquelas que seriam registradas nos níveis mais altos. Por exemplo, o nível Normal inclui todas as mensagens de erro.

Se você não precisar de um registro detalhado das operações de leitura do cliente para seus aplicativos S3, opcionalmente, altere a configuração **Leituras do cliente** para **Erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria.

3. Selecione **Salvar**.

   Um banner verde indica que sua configuração foi salva.

Definir cabeçalhos de solicitação HTTP

Opcionalmente, você pode definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente. Esses cabeçalhos de protocolo se aplicam somente a solicitações S3.

Passos

1. Na seção **Cabeçalhos do protocolo de auditoria**, defina os cabeçalhos de solicitação HTTP que você deseja incluir nas mensagens de auditoria de leitura e gravação do cliente.

   Use um asterisco (*) como curinga para corresponder a zero ou mais caracteres. Use a sequência de escape (*) para corresponder a um asterisco literal.

2. Selecione **Adicionar outro cabeçalho** para criar cabeçalhos adicionais, se necessário.

   Quando cabeçalhos HTTP são encontrados em uma solicitação, eles são incluídos na mensagem de auditoria no campo HTRH.

   Os cabeçalhos de solicitação do protocolo de auditoria serão registrados somente se o nível de auditoria para **Leituras do cliente** ou **Gravações do cliente** não for **Desativado**.

3. Selecione **Salvar**

   Um banner verde indica que sua configuração foi salva.

Use um servidor syslog externo

Opcionalmente, você pode configurar um servidor syslog externo para salvar logs de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora da sua grade.

Se você não quiser usar um servidor syslog externo, pule esta etapa e vá paraSelecione destinos de informações de auditoria .

Se as opções de configuração disponíveis neste procedimento não forem flexíveis o suficiente para atender às suas necessidades, opções de configuração adicionais podem ser aplicadas usando o `audit-destinations` endpoints, que estão na seção de API privada do"API de gerenciamento de grade" . Por exemplo, você pode usar a API se quiser usar diferentes servidores syslog para diferentes grupos de nós.

Insira as informações do syslog

Acesse o assistente Configurar servidor syslog externo e forneça as informações que o StorageGRID precisa para acessar o servidor syslog externo.

Passos

1. Na página Auditoria e servidor syslog, selecione **Configurar servidor syslog externo**. Ou, se você configurou anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

   O assistente Configurar servidor syslog externo é exibido.

2. Para a etapa **Inserir informações do syslog** do assistente, insira um nome de domínio totalmente qualificado válido ou um endereço IPv4 ou IPv6 para o servidor syslog externo no campo **Host**.
3. Insira a porta de destino no servidor syslog externo (deve ser um número inteiro entre 1 e 65535). A porta padrão é 514.
4. Selecione o protocolo usado para enviar informações de auditoria para o servidor syslog externo.

   É recomendado usar **TLS** ou **RELP/TLS**. Você deve carregar um certificado de servidor para usar qualquer uma dessas opções. O uso de certificados ajuda a proteger as conexões entre sua grade e o servidor syslog externo. Para obter mais informações, consulte "Gerenciar certificados de segurança" .

   Todas as opções de protocolo exigem suporte e configuração do servidor syslog externo. Você deve escolher uma opção compatível com o servidor syslog externo.

   > ⓘ O Reliable Event Logging Protocol (RELP) estende a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. Usar o RELP pode ajudar a evitar a perda de informações de auditoria caso seu servidor syslog externo precise reiniciar.

5. Selecione **Continuar**.
6. Se você selecionou **TLS** ou **RELP/TLS**, carregue os certificados da CA do servidor, o certificado do cliente e a chave privada do cliente.
   a. Selecione **Procurar** para o certificado ou chave que você deseja usar.
   b. Selecione o certificado ou arquivo de chave.
   c. Selecione **Abrir** para carregar o arquivo.

      Uma marca de verificação verde aparece ao lado do nome do certificado ou do arquivo de chave, notificando que ele foi carregado com sucesso.

7. Selecione **Continuar**.

Gerenciar conteúdo do syslog

Você pode selecionar quais informações enviar para o servidor syslog externo.

Passos

1. Para a etapa **Gerenciar conteúdo do syslog** do assistente, selecione cada tipo de informação de auditoria que deseja enviar ao servidor syslog externo.
   - **Enviar logs de auditoria**: Envia eventos do StorageGRID e atividades do sistema
   - **Enviar eventos de segurança**: Envia eventos de segurança, como quando um usuário não autorizado tenta fazer login ou um usuário faz login como root
   - **Enviar logs de aplicação**: Envia"Arquivos de log do software StorageGRID" útil para solução de problemas, incluindo:
     - `bycast-err.log`

- `bycast.log`
- `jaeger.log`
- `nms.log`(Somente nós de administração)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

◦ **Enviar logs de acesso**: Envia logs de acesso HTTP para solicitações externas ao Grid Manager, Tenant Manager, endpoints de balanceador de carga configurados e solicitações de federação de grade de sistemas remotos.

2. Use os menus suspensos para selecionar a gravidade e a facilidade (tipo de mensagem) para cada categoria de informação de auditoria que você deseja enviar.

   Definir valores de gravidade e facilidade pode ajudar você a agregar os logs de maneiras personalizáveis para facilitar a análise.

   a. Para **Gravidade**, selecione **Passagem** ou selecione um valor de gravidade entre 0 e 7.

      Se você selecionar um valor, o valor selecionado será aplicado a todas as mensagens deste tipo. Informações sobre diferentes gravidades serão perdidas se você substituir a gravidade por um valor fixo.

Gravidade	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de gravidade de quando foi registrada localmente no nó: • Para logs de auditoria, a gravidade é "info". • Para eventos de segurança, os valores de gravidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, as gravidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA fornece um valor de "info", enquanto interromper intencionalmente o serviço SSM ou RSM fornece um valor de "notice". • Para logs de acesso, a gravidade é "info".
0	Emergência: O sistema está inutilizável
1	Alerta: Ação deve ser tomada imediatamente
2	Crítico: Condições críticas
3	Erro: Condições de erro
4	Aviso: Condições de aviso

Gravidade	Descrição
5	Aviso: Condição normal, mas significativa
6	Informativo: Mensagens informativas
7	Depuração: mensagens de nível de depuração

b. Para **Instalação**, selecione **Passthrough** ou selecione um valor de instalação entre 0 e 23.

Se você selecionar um valor, ele será aplicado a todas as mensagens deste tipo. Informações sobre diferentes instalações serão perdidas se você substituir a instalação por um valor fixo.

Instalação	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de recurso de quando foi registrada localmente no nó: • Para logs de auditoria, o recurso enviado ao servidor syslog externo é "local7". • Para eventos de segurança, os valores de facilidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados ao servidor syslog externo têm os seguintes valores de facilidade: ◦ `bycast.log`: usuário ou daemon ◦ `bycast-err.log`: usuário, daemon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Para logs de acesso, o recurso enviado ao servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	usuário (mensagens em nível de usuário)
2	correspondência
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)

Instalação	Descrição
5	syslog (mensagens geradas internamente pelo syslogd)
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias da rede)
8	UUCP
9	cron (daemon do relógio)
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (auditoria de log)
14	logalert (alerta de registro)
15	relógio (daemon do relógio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selecione **Continuar**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós na sua grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para

ajudar a validar toda a sua infraestrutura de coleta de logs antes de se comprometer a enviar dados para o servidor syslog externo.

> Não use a configuração do servidor syslog externo até confirmar que o servidor syslog externo recebeu uma mensagem de teste de cada nó na sua grade e que a mensagem foi processada conforme o esperado.

Passos

1. Se você não quiser enviar mensagens de teste porque tem certeza de que seu servidor syslog externo está configurado corretamente e pode receber informações de auditoria de todos os nós em sua grade, selecione **Ignorar e concluir**.

   Um banner verde indica que a configuração foi salva.

2. Caso contrário, selecione **Enviar mensagens de teste** (recomendado).

   Os resultados dos testes aparecem continuamente na página até você interromper o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuarão sendo enviadas para os destinos configurados anteriormente.

3. Se você receber algum erro durante a configuração do servidor syslog ou em tempo de execução, corrija-o e selecione **Enviar mensagens de teste** novamente.

   Ver"Solucionar problemas de um servidor syslog externo" para ajudar você a resolver quaisquer erros.

4. Aguarde até ver um banner verde indicando que todos os nós passaram no teste.
5. Verifique seu servidor syslog para determinar se as mensagens de teste estão sendo recebidas e processadas conforme o esperado.

   > Se você estiver usando UDP, verifique toda a sua infraestrutura de coleta de logs. O protocolo UDP não permite uma detecção de erros tão rigorosa quanto os outros protocolos.

6. Selecione **Parar e finalizar**.

   Você retornará à página **Auditoria e servidor syslog**. Um banner verde indica que a configuração do servidor syslog foi salva.

   > As informações de auditoria do StorageGRID não são enviadas ao servidor syslog externo até que você selecione um destino que inclua o servidor syslog externo.

Selecione destinos de informações de auditoria

Você pode especificar onde os logs de auditoria, logs de eventos de segurança e"Registros do software StorageGRID" são enviados.

O StorageGRID assume como padrão os destinos de auditoria de nós locais e armazena as informações de auditoria em `/var/local/log/localaudit.log`.

Ao usar `/var/local/log/localaudit.log`, as entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de armazenamento. Você pode descobrir qual nó tem as entradas mais recentes usando o `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

Alguns destinos só estarão disponíveis se você tiver configurado um servidor syslog externo.

Passos

1. Na página Auditoria e servidor syslog, selecione o destino para as informações de auditoria.

Somente nós locais e **servidor syslog externo** geralmente oferecem melhor desempenho.

Opção	Descrição
Somente nós locais (padrão)	Mensagens de auditoria, logs de eventos de segurança e logs de aplicativos não são enviados aos nós de administração. Em vez disso, eles são salvos apenas nos nós que os geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas em `/var/local/log/localaudit.log`. **Observação**: O StorageGRID remove periodicamente logs locais em uma rotação para liberar espaço. Quando o arquivo de log de um nó atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado. O limite de rotação do log é de 21 arquivos. Quando a 22ª versão do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó.
Nós de administração/nós locais	As mensagens de auditoria são enviadas para o log de auditoria nos nós de administração, e os logs de eventos de segurança e logs de aplicativos são armazenados nos nós que os geraram. As informações de auditoria são armazenadas nos seguintes arquivos: • Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` o arquivo normalmente está vazio ou ausente. Pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais(`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção é habilitada somente após você configurar um servidor syslog externo.

Opção	Descrição
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria(`/var/local/audit/export/audit.log`) em nós de administração, e as informações de auditoria são enviadas ao servidor syslog externo e salvas no nó local(`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção é habilitada somente após você configurar um servidor syslog externo.

2. Selecione **Salvar**.

   Uma mensagem de aviso é exibida.

3. Selecione **OK** para confirmar que deseja alterar o destino das informações de auditoria.

   Um banner verde indica que a configuração de auditoria foi salva.

   Novos logs são enviados para os destinos selecionados. Os registros existentes permanecem em seu local atual.

Usar monitoramento SNMP

Usar monitoramento SNMP

Se você quiser monitorar o StorageGRID usando o Protocolo Simples de Gerenciamento de Rede (SNMP), deverá configurar o agente SNMP incluído no StorageGRID.

- "Configurar o agente SNMP"
- "Atualizar o agente SNMP"

Capacidades

Cada nó StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB StorageGRID contém definições de tabela e notificação para alertas. O MIB também contém informações de descrição do sistema, como plataforma e número do modelo para cada nó. Cada nó StorageGRID também suporta um subconjunto de objetos MIB-II.

Ver"Acessar arquivos MIB" se você quiser baixar os arquivos MIB nos nós da sua grade.

Inicialmente, o SNMP é desabilitado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Ele fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

Armadilhas

Armadilhas são notificações enviadas pelo agente SNMP que não exigem confirmação pelo sistema de gerenciamento. As armadilhas servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como um alerta sendo disparado.

As armadilhas são suportadas em todas as três versões do SNMP.

Informa

As informações são semelhantes às armadilhas, mas exigem reconhecimento pelo sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará a informação até que uma confirmação seja recebida ou o valor máximo de novas tentativas seja atingido.

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de captura e informação são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP para um alerta, você deve"configurar um silêncio" para o alerta. As notificações de alerta são enviadas pelo"nó de administração do remetente preferencial" .

  Cada alerta é mapeado para um dos três tipos de armadilhas com base no nível de gravidade do alerta: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem disparar essas armadilhas, consulte o"Referência de alertas" .

Suporte à versão SNMP

A tabela fornece um resumo de alto nível do que é suportado para cada versão do SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de caracteres da comunidade	Cadeia de caracteres da comunidade	Usuário do Modelo de Segurança Baseado no Usuário (USM)
Notificações (ARMAZENAR e INFORMAR)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Usuário USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.

- SNMPv3: O StorageGRID não oferece suporte ao Modo de Suporte de Transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é o SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é o AES.

Configurar o agente SNMP

Você pode configurar o agente SNMP do StorageGRID para usar um sistema de gerenciamento SNMP de terceiros para acesso MIB somente leitura e notificações.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

O agente SNMP do StorageGRID oferece suporte a SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, somente a autenticação do Modelo de Segurança do Usuário (USM) é suportada.

Todos os nós na grade usam a mesma configuração SNMP.

Especificar configuração básica

Como primeiro passo, habilite o agente StorageGRID SMNP e forneça informações básicas.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.

   A página do agente SNMP é exibida.

2. Para habilitar o agente SNMP em todos os nós da grade, marque a caixa de seleção **Habilitar SNMP**.
3. Insira as seguintes informações na seção Configuração básica.

Campo	Descrição
Contato do sistema	Opcional. O contato principal do sistema StorageGRID , que é retornado em mensagens SNMP como sysContact. O contato do sistema normalmente é um endereço de e-mail. Este valor se aplica a todos os nós no sistema StorageGRID . **Contato do sistema** pode ter no máximo 255 caracteres.
Localização do sistema	Opcional. A localização do sistema StorageGRID , que é retornada em mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde seu sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço de uma instalação. Este valor se aplica a todos os nós no sistema StorageGRID . **Localização do sistema** pode ter no máximo 255 caracteres.

Campo	Descrição
Habilitar notificações do agente SNMP	• Se selecionado, o agente SNMP StorageGRID envia notificações de interceptação e informação. • Se não for selecionado, o agente SNMP suportará acesso MIB somente leitura, mas não enviará nenhuma notificação SNMP.
Habilitar armadilhas de autenticação	Se selecionado, o agente SNMP do StorageGRID enviará interceptações de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Insira as sequências da comunidade

Se você usar SNMPv1 ou SNMPv2c, preencha a seção Strings da comunidade.

Quando o sistema de gerenciamento consulta o StorageGRID MIB, ele envia uma string de comunidade. Se a sequência de caracteres da comunidade corresponder a um dos valores especificados aqui, o agente SNMP enviará uma resposta ao sistema de gerenciamento.

Passos

1. Para **Comunidade somente leitura**, insira opcionalmente uma sequência de caracteres de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6.

   Para garantir a segurança do seu sistema StorageGRID , não use "public" como string de comunidade. Se você deixar este campo em branco, o agente SNMP usará o ID da grade do seu sistema StorageGRID como a string da comunidade.

   Cada sequência de caracteres da comunidade pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Selecione **Adicionar outra sequência de comunidade** para adicionar sequências adicionais.

   São permitidas até cinco strings.

Criar destinos de armadilha

Use a guia Destinos de interceptação na seção Outras configurações para definir um ou mais destinos para interceptação do StorageGRID ou informar notificações. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Passos

1. Para o campo **Comunidade de interceptação padrão**, insira opcionalmente a sequência de caracteres da comunidade padrão que você deseja usar para destinos de interceptação SNMPv1 ou SNMPv2.

   Conforme necessário, você pode fornecer uma sequência de caracteres de comunidade diferente ("personalizada") ao definir um destino de captura específico.

   Comunidade de trap padrão pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Para adicionar um destino de armadilha, selecione **Criar**.
3. Selecione qual versão SNMP será usada para este destino de trap.
4. Preencha o formulário Criar destino de armadilha para a versão selecionada.

SNMPv1

Se você selecionou SNMPv1 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Deve ser Trap para SNMPv1.
Hospedar	Um endereço IPv4 ou IPv6 ou um nome de domínio totalmente qualificado (FQDN) para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv2c

Se você selecionou SNMPv2c como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv3

Se você selecionou SNMPv3 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Usuário USM	O usuário USM que será usado para autenticação. • Se você selecionou **Trap**, somente usuários do USM sem IDs de mecanismo autoritativos serão exibidos. • Se você selecionou **Informar**, somente usuários do USM com IDs de mecanismo autoritativos serão exibidos. • Se nenhum usuário for exibido: i. Crie e salve o destino da armadilha. ii. Vá paraCriar usuários USM e criar o usuário. iii. Retorne à aba Destinos da armadilha, selecione o destino salvo na tabela e selecione **Editar**. iv. Selecione o usuário.

5. Selecione **Criar**.

   O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agentes

Opcionalmente, use a guia Endereços do agente na seção Outras configurações para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Se você não configurar um endereço de agente, o endereço de escuta padrão será a porta UDP 161 em todas as redes StorageGRID .

Passos

1. Selecione **Criar**.
2. Insira as seguintes informações.

Campo	Descrição
Protocolo de internet	Se este endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se este endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Em qual rede StorageGRID o agente irá escutar. • Redes de grade, administração e cliente: o agente SNMP escutará consultas em todas as três redes. • Rede de grade • Rede de administração • Rede de clientes **Observação**: se você usar a Rede do Cliente para dados inseguros e criar um endereço de agente para a Rede do Cliente, esteja ciente de que o tráfego SNMP também será inseguro.
Porta	Opcionalmente, o número da porta na qual o agente SNMP deve escutar. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Observação**: quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

3. Selecione **Criar**.

   O endereço do agente é criado e adicionado à tabela.

Criar usuários USM

Se você estiver usando SNMPv3, use a guia Usuários do USM na seção Outras configurações para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber traps e informações.

> Os destinos SNMPv3 *inform* devem ter usuários com IDs de mecanismo. O destino SNMPv3 *trap* não pode ter usuários com IDs de mecanismo.

Essas etapas não se aplicam se você estiver usando apenas SNMPv1 ou SNMPv2c.

Passos

1. Selecione **Criar**.

2. Insira as seguintes informações.

Campo	Descrição
Nome de usuário	Um nome exclusivo para este usuário USM. Os nomes de usuário podem ter no máximo 32 caracteres e não podem conter espaços em branco. O nome de usuário não pode ser alterado após a criação do usuário.
Acesso MIB somente leitura	Se selecionado, este usuário deverá ter acesso somente leitura ao MIB.
ID do mecanismo autoritativo	Se este usuário for usado em um destino de informação, o ID do mecanismo autoritativo para este usuário. Digite de 10 a 64 caracteres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para usuários do USM que serão selecionados em destinos de trap para informações. Este valor não é permitido para usuários do USM que serão selecionados em destinos de armadilhas para armadilhas. **Observação**: Este campo não será exibido se você selecionar **Acesso MIB somente leitura** porque os usuários do USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o usuário USM: • **authPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Você deve especificar um protocolo de autenticação e uma senha, bem como um protocolo de privacidade e uma senha. • **authNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Você deve especificar um protocolo de autenticação e uma senha.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Senha	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Exibido somente se você selecionou **authPriv** e sempre definiu como AES, que é o único protocolo de privacidade suportado.
Senha	Exibido somente se você selecionou **authPriv**. A senha que este usuário usará para privacidade.

3. Selecione **Criar**.

   O usuário USM é criado e adicionado à tabela.

4. Quando tiver concluído a configuração do agente SNMP, selecione **Salvar**.

   A nova configuração do agente SNMP fica ativa.

Atualizar o agente SNMP

Você pode desabilitar notificações SNMP, atualizar strings de comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de interceptação.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

Ver"Configurar o agente SNMP" para obter detalhes sobre cada campo na página do agente SNMP. Você deve selecionar **Salvar** na parte inferior da página para confirmar quaisquer alterações feitas em cada guia.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.

   A página do agente SNMP é exibida.

2. Para desabilitar o agente SNMP em todos os nós da grade, desmarque a caixa de seleção **Habilitar SNMP** e selecione **Salvar**.

   Se você reativar o agente SNMP, todas as configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize as informações na seção Configuração básica:
   a. Conforme necessário, atualize o **Contato do sistema** e o **Local do sistema**.
   b. Opcionalmente, marque ou desmarque a caixa de seleção **Habilitar notificações do agente SNMP** para controlar se o agente SNMP do StorageGRID envia notificações de interceptação e informação.

      Quando esta caixa de seleção está desmarcada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

   c. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar armadilhas de autenticação** para controlar se o agente SNMP do StorageGRID envia armadilhas de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usar SNMPv1 ou SNMPv2c, opcionalmente atualize ou adicione uma **Comunidade somente leitura** na seção Strings da comunidade.
5. Para atualizar destinos de armadilhas, selecione a aba Destinos de armadilhas na seção Outras configurações.

   Use esta guia para definir um ou mais destinos para notificações de interceptação ou informação do StorageGRID . Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

   Para obter detalhes sobre o que inserir, consulte"Criar destinos de armadilhas" .

   - Opcionalmente, atualize ou remova a comunidade de armadilhas padrão.

Se você remover a comunidade de armadilhas padrão, primeiro deverá garantir que todos os destinos de armadilhas existentes usem uma sequência de caracteres de comunidade personalizada.

- Para adicionar um destino de armadilha, selecione **Criar**.
- Para editar um destino de armadilha, selecione o botão de opção e selecione **Editar**.
- Para remover um destino de armadilha, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

6. Para atualizar endereços de agentes, selecione a guia Endereços de agentes na seção Outras configurações.

   Use esta aba para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

   Para obter detalhes sobre o que inserir, consulte"Criar endereços de agentes" .

   - Para adicionar um endereço de agente, selecione **Criar**.
   - Para editar o endereço de um agente, selecione o botão de opção e selecione **Editar**.
   - Para remover um endereço de agente, selecione o botão de opção e selecione **Remover**.
   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

7. Para atualizar usuários do USM, selecione a guia Usuários do USM na seção Outras configurações.

   Use esta guia para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber armadilhas e informações.

   Para obter detalhes sobre o que inserir, consulte"Criar usuários USM" .

   - Para adicionar um usuário USM, selecione **Criar**.
   - Para editar um usuário USM, selecione o botão de opção e selecione **Editar**.

     O nome de usuário de um usuário USM existente não pode ser alterado. Se precisar alterar um nome de usuário, você deverá removê-lo e criar um novo.

     > Se você adicionar ou remover o ID de mecanismo autoritativo de um usuário e esse usuário estiver selecionado para um destino, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

   - Para remover um usuário do USM, selecione o botão de opção e selecione **Remover**.

     > Se o usuário que você removeu estiver selecionado para um destino de interceptação, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando você tiver atualizado a configuração do agente SNMP, selecione **Salvar**.

Acessar arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e serviços gerenciados para os nós na sua grade. Você pode acessar arquivos MIB que

definem os objetos e notificações para StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Ver"Usar monitoramento SNMP" para mais informações sobre arquivos SNMP e MIB.

Acessar arquivos MIB

Siga estas etapas para acessar os arquivos MIB.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.
2. Na página do agente SNMP, selecione o arquivo que deseja baixar:
   - **NETAPP-STORAGEGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os nós de administração.
   - **ES-NETAPP-06-MIB.mib**: Define objetos e notificações para dispositivos baseados na Série E.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com uma interface BMC .

   > Você também pode acessar arquivos MIB no seguinte local em qualquer nó do StorageGRID : `/usr/share/snmp/mibs`

3. Para extrair os OIDs do StorageGRID do arquivo MIB:
   a. Obtenha o OID da raiz do StorageGRID MIB:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Resultado: `.1.3.6.1.4.1.789.28669` (`28669` é sempre o OID para StorageGRID)

   a. Grep para o OID StorageGRID em toda a árvore (usando `paste` para unir linhas):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

> O `snmptranslate` O comando tem muitas opções úteis para explorar o MIB. Este comando está disponível em qualquer nó StorageGRID .

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID StorageGRID .

Nome do objeto	ID do objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID .

Objetos MIB

Nome do objeto	ID do objeto (OID)	Descrição
Contagem de Alerta Ativo		O número de alertas ativos na activeAlertTable.
Tabela de Alerta Ativo		Uma tabela de alertas ativos no StorageGRID.
ID de alerta ativo		O ID do alerta. Único no conjunto atual de alertas ativos.
NomeAlertaAtivo		O nome do alerta.
instância de alerta ativo		O nome da entidade que gerou o alerta, normalmente o nome do nó.
activeAlertSeverity		A gravidade do alerta.
hora de início do alerta ativo		Data e hora em que o alerta foi disparado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ID de alerta ativo
- NomeAlertaAtivo
- instância de alerta ativo
- activeAlertSeverity
- hora de início do alerta ativo

Tipo de notificação	ID do objeto (OID)	Descrição
Alerta Menor Ativo		Um alerta com gravidade menor
AlertaMaiorAtivo		Um alerta com grande gravidade
AlertaCríticoAtivo		Um alerta com gravidade crítica

Coletar dados adicionais do StorageGRID

Use tabelas e gráficos

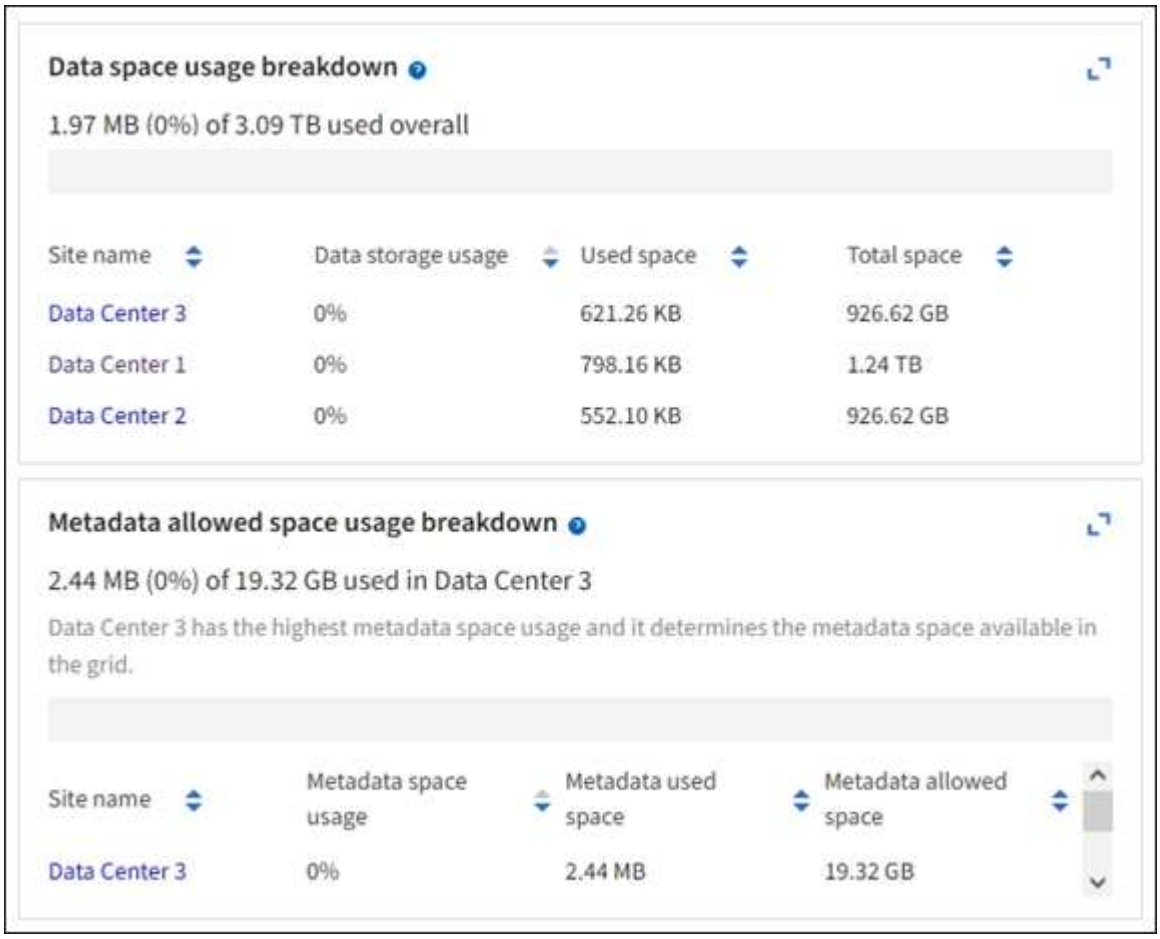
Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas.

O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

Tipos de gráficos

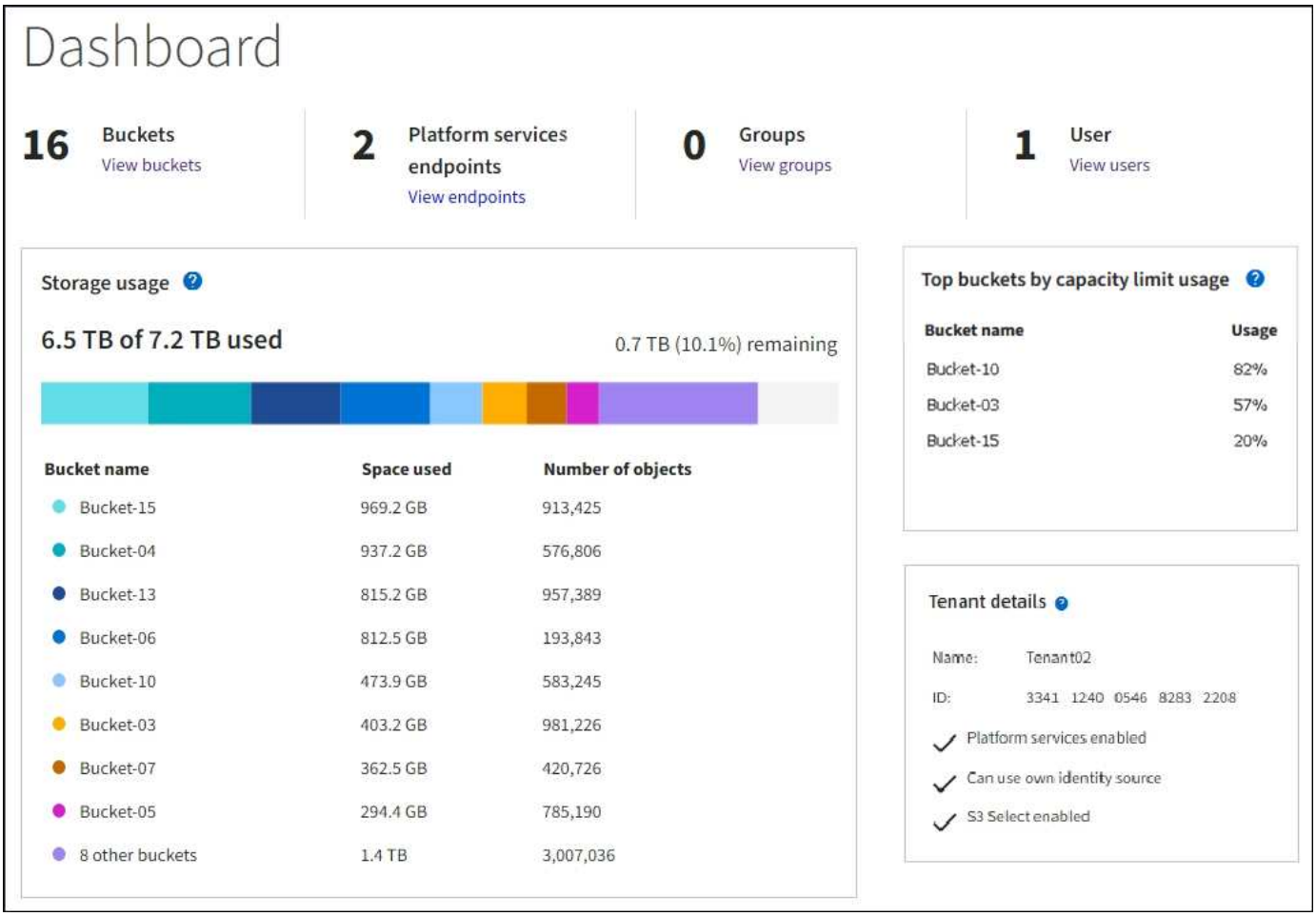
Gráficos e tabelas resumem os valores de métricas e atributos específicos do StorageGRID .

O painel do Grid Manager inclui cartões que resumem o armazenamento disponível para a grade e cada site.



O painel de uso de armazenamento no painel do Gerenciador de locatários exibe o seguinte:

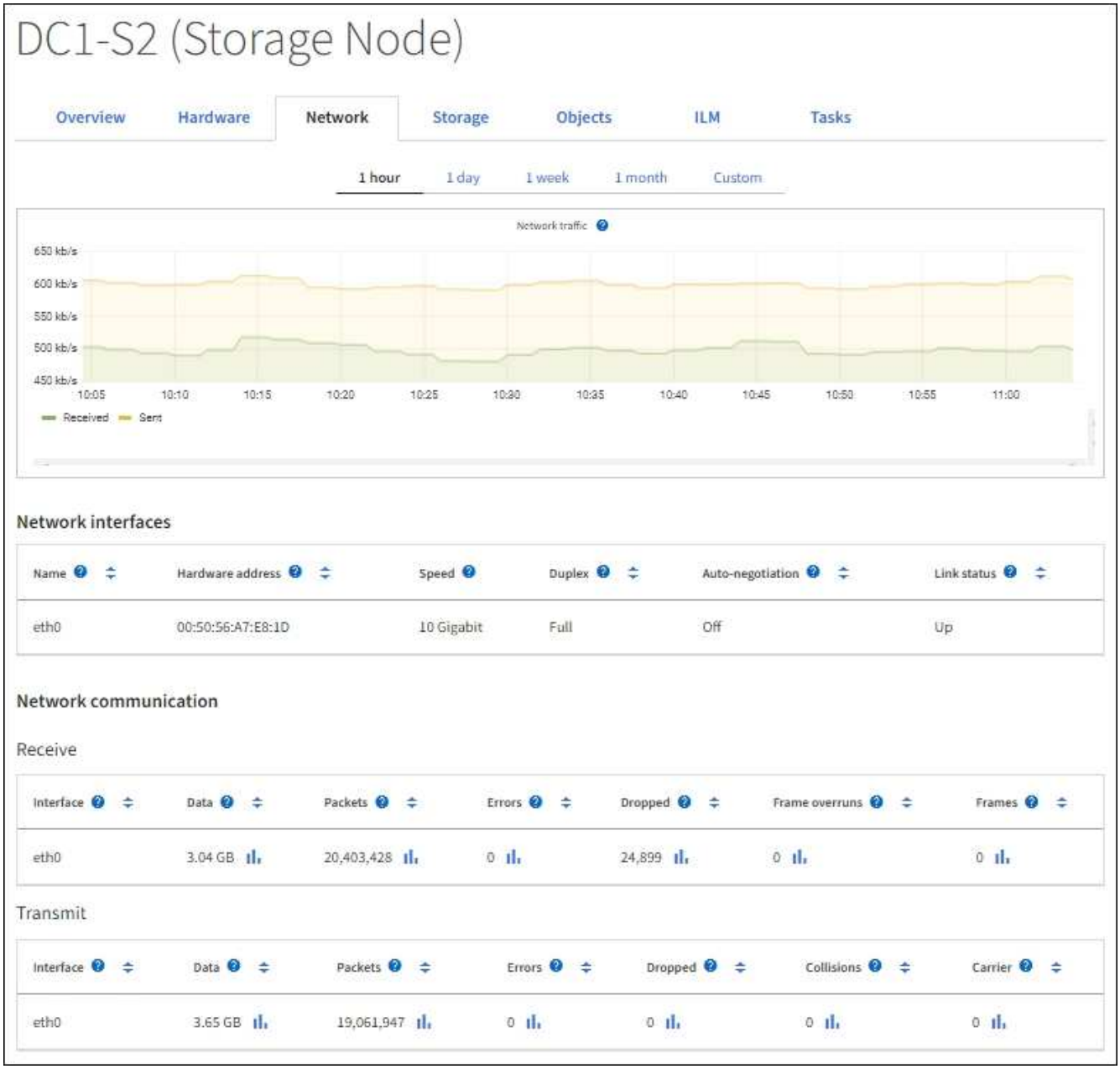
- Uma lista dos maiores buckets (S3) ou contêineres (Swift) para o locatário
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou recipientes
- A quantidade total de espaço utilizado e, se uma cota for definida, a quantidade e a porcentagem de espaço restante



Além disso, gráficos que mostram como as métricas e os atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página Nós e na página **SUPORTE** > **Ferramentas** > **Topologia de grade**.

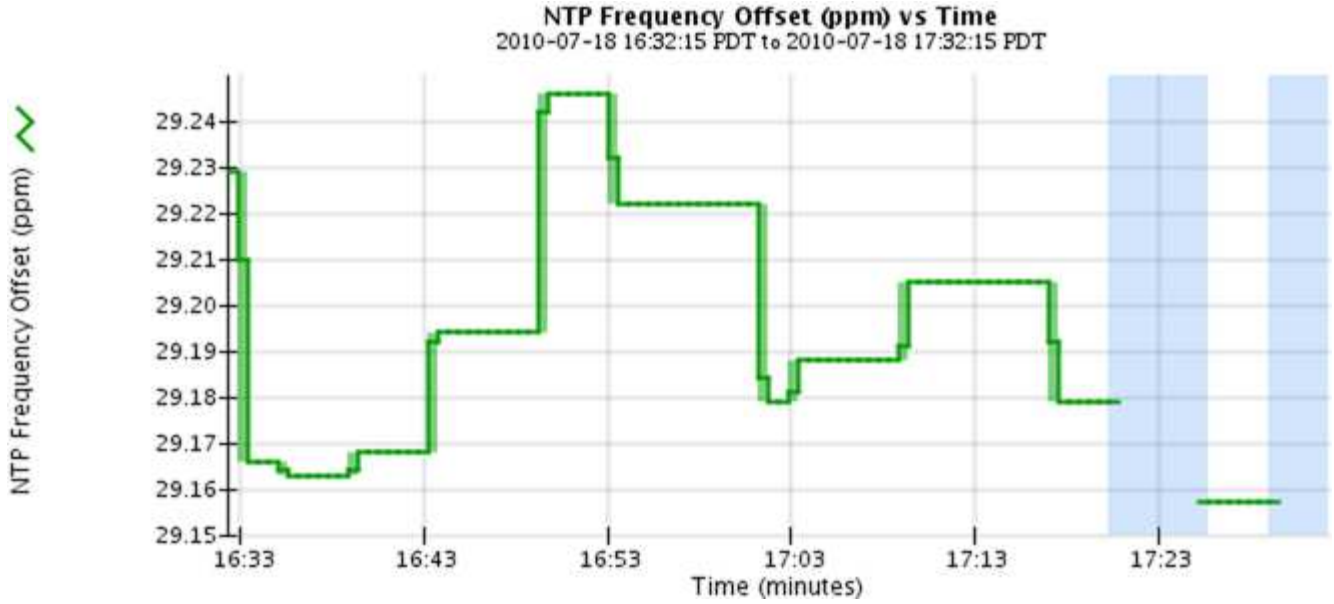
Existem quatro tipos de gráficos:

- **Gráficos Grafana**: Exibidos na página Nós, os gráficos Grafana são usados para plotar os valores das métricas do Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **Rede** para um Nó de Armazenamento inclui um gráfico Grafana para tráfego de rede.

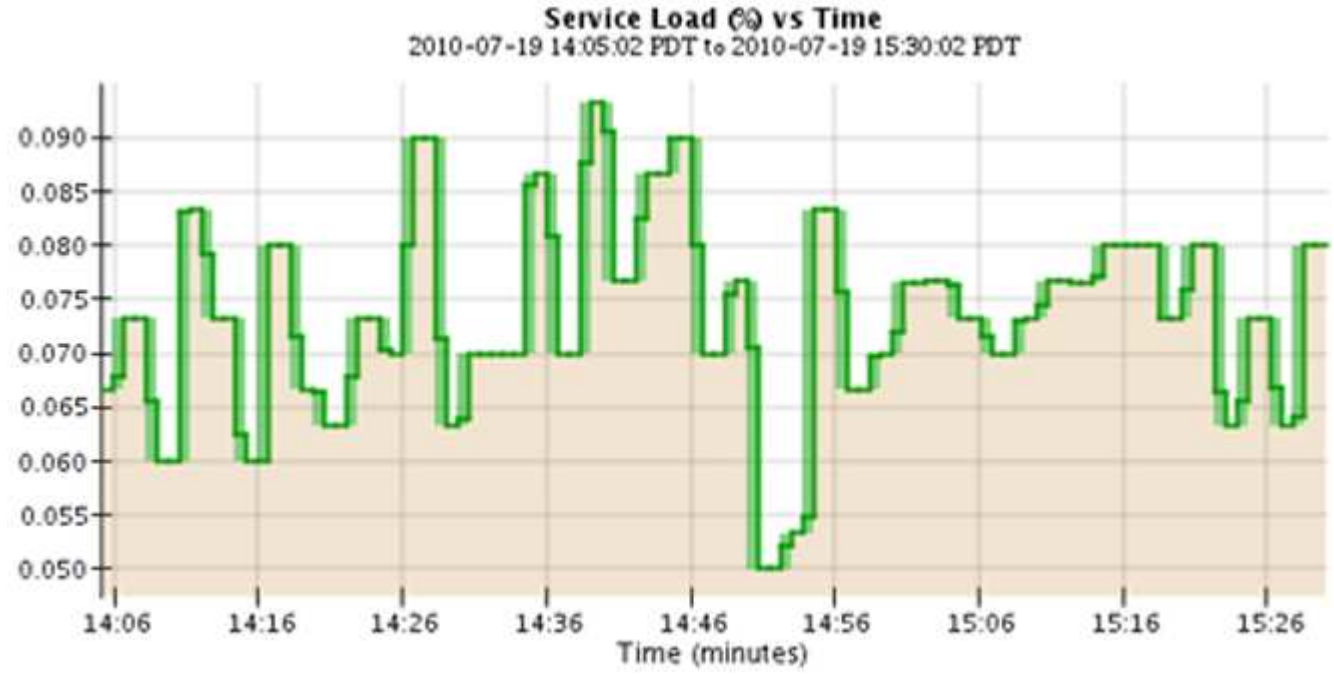


Os gráficos do Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPORTE** > **Ferramentas** > **Métricas**.

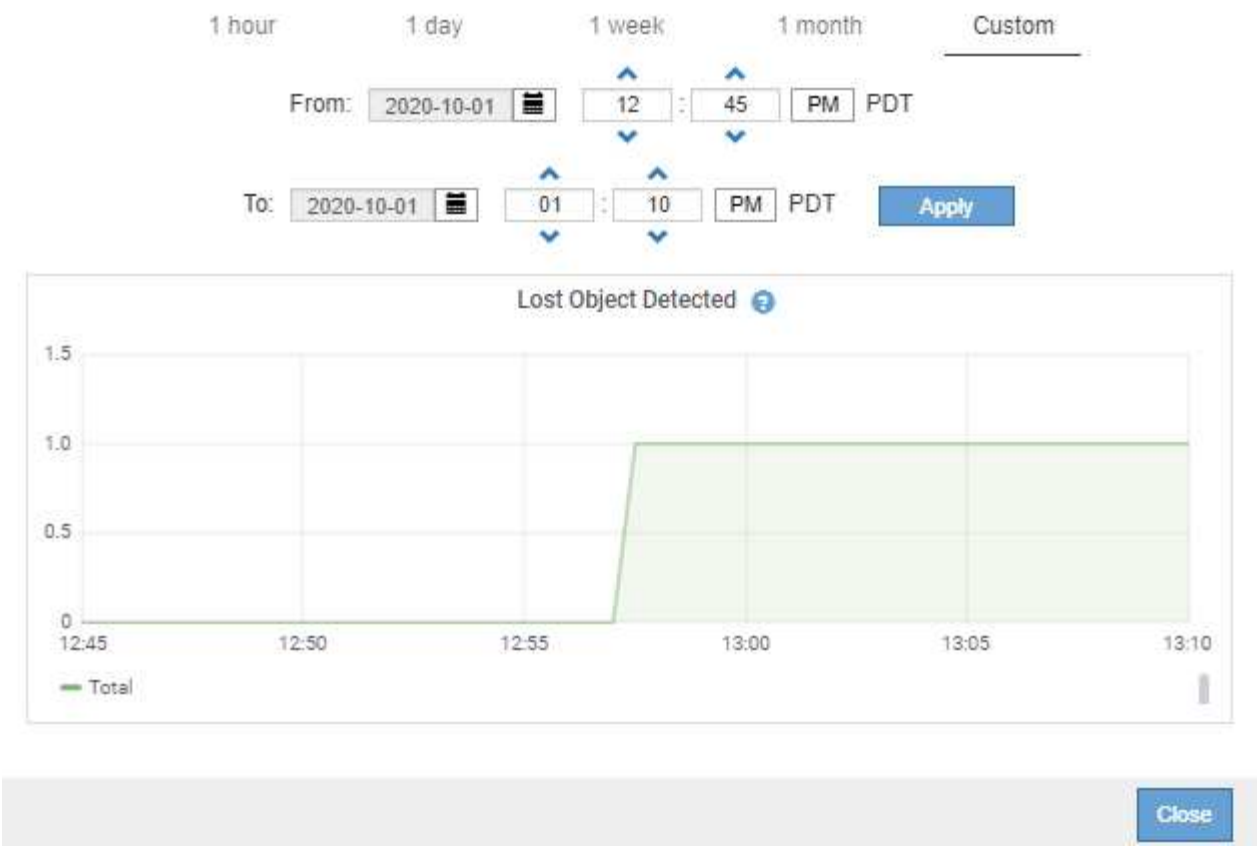
- **Gráficos de linha**: Disponíveis na página Nós e na página **SUPORTE** > **Ferramentas** > **Topologia de grade** (selecione o ícone do gráfico após um valor de dados), gráficos de linha são usados para plotar os valores dos atributos StorageGRID que têm um valor unitário (como deslocamento de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



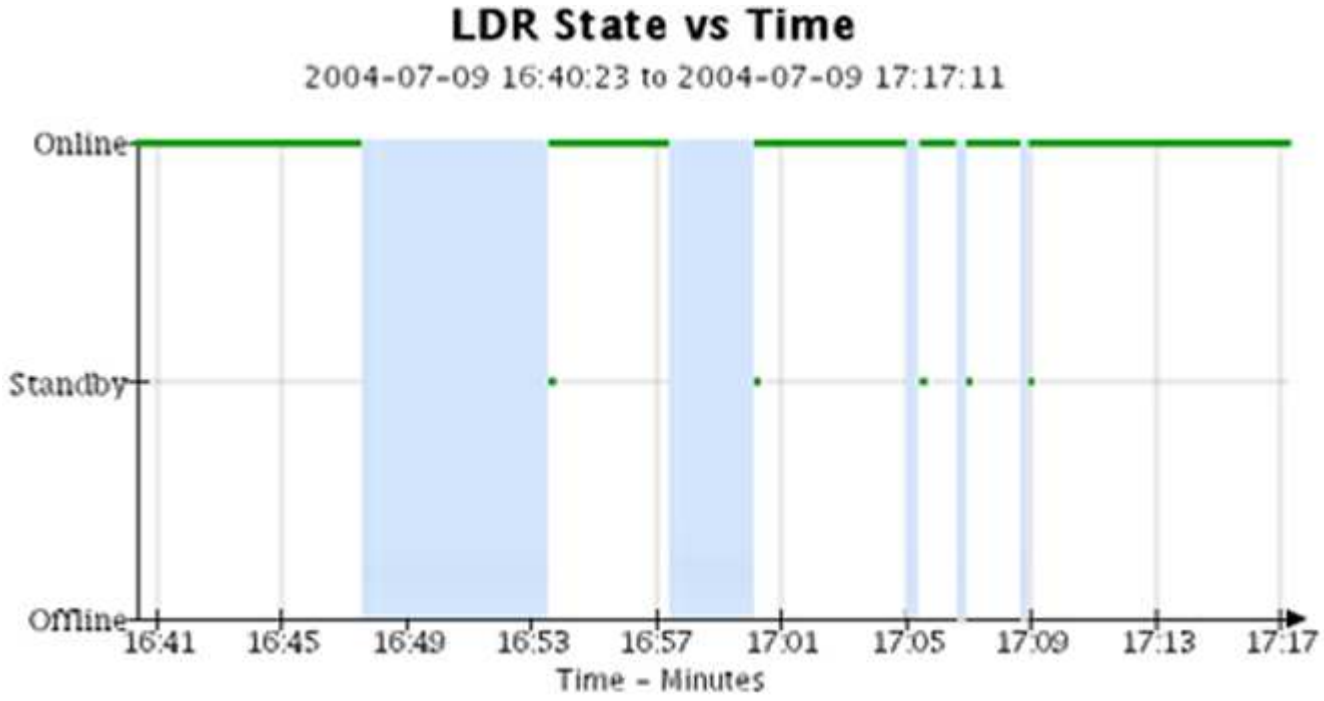
- **Gráficos de área**: Disponíveis na página Nós e na página **SUPORTE** > **Ferramentas** > **Topologia de grade** (selecione o ícone do gráfico após um valor de dados), gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. Os gráficos de área são semelhantes aos gráficos de linhas, mas incluem um sombreamento marrom claro abaixo da linha. As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



- Alguns gráficos são indicados com um tipo diferente de ícone de gráfico e têm um formato diferente:



- **Gráfico de estado**: Disponível na página **SUPORTE** > **Ferramentas** > **Topologia de grade** (selecione o ícone do gráfico após um valor de dados), os gráficos de estado são usados para plotar valores de atributos que representam estados distintos, como um estado de serviço que pode ser online, em espera ou offline. Os gráficos de estado são semelhantes aos gráficos de linha, mas a transição é descontínua; ou seja, o valor salta de um valor de estado para outro.

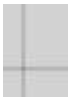


Informações relacionadas

- "Ver a página de nós"
- "Visualizar a árvore de topologia da grade"
- "Revisar métricas de suporte"

Legenda do gráfico

As linhas e cores usadas para desenhar gráficos têm um significado específico.

Exemplo	Significado
	Os valores de atributos relatados são plotados usando linhas verde-escuras.
	O sombreamento verde claro ao redor das linhas verde escuro indica que os valores reais nesse intervalo de tempo variam e foram "agrupados" para uma plotagem mais rápida. A linha escura representa a média ponderada. O intervalo em verde claro indica os valores máximo e mínimo dentro do compartimento. O sombreamento marrom claro é usado em gráficos de área para indicar dados volumétricos.
	Áreas em branco (sem dados plotados) indicam que os valores dos atributos não estavam disponíveis. O fundo pode ser azul, cinza ou uma mistura de cinza e azul, dependendo do estado do serviço que relata o atributo.
	O sombreamento azul claro indica que alguns ou todos os valores de atributo naquele momento eram indeterminados; o atributo não estava relatando valores porque o serviço estava em um estado desconhecido.
	O sombreamento cinza indica que alguns ou todos os valores de atributos naquele momento não eram conhecidos porque o serviço que relatava os atributos estava administrativamente inativo.
	Uma mistura de sombreamento cinza e azul indica que alguns dos valores de atributos no momento eram indeterminados (porque o serviço estava em um estado desconhecido), enquanto outros não eram conhecidos porque o serviço que relatava os atributos estava administrativamente inativo.

Exibir tabelas e gráficos

A página Nós contém os gráficos e tabelas que você deve acessar regularmente para monitorar atributos como capacidade de armazenamento e taxa de transferência. Em alguns casos, especialmente ao trabalhar com suporte técnico, você pode usar a página **SUPORTE** > **Ferramentas** > **Topologia de grade** para acessar gráficos adicionais.

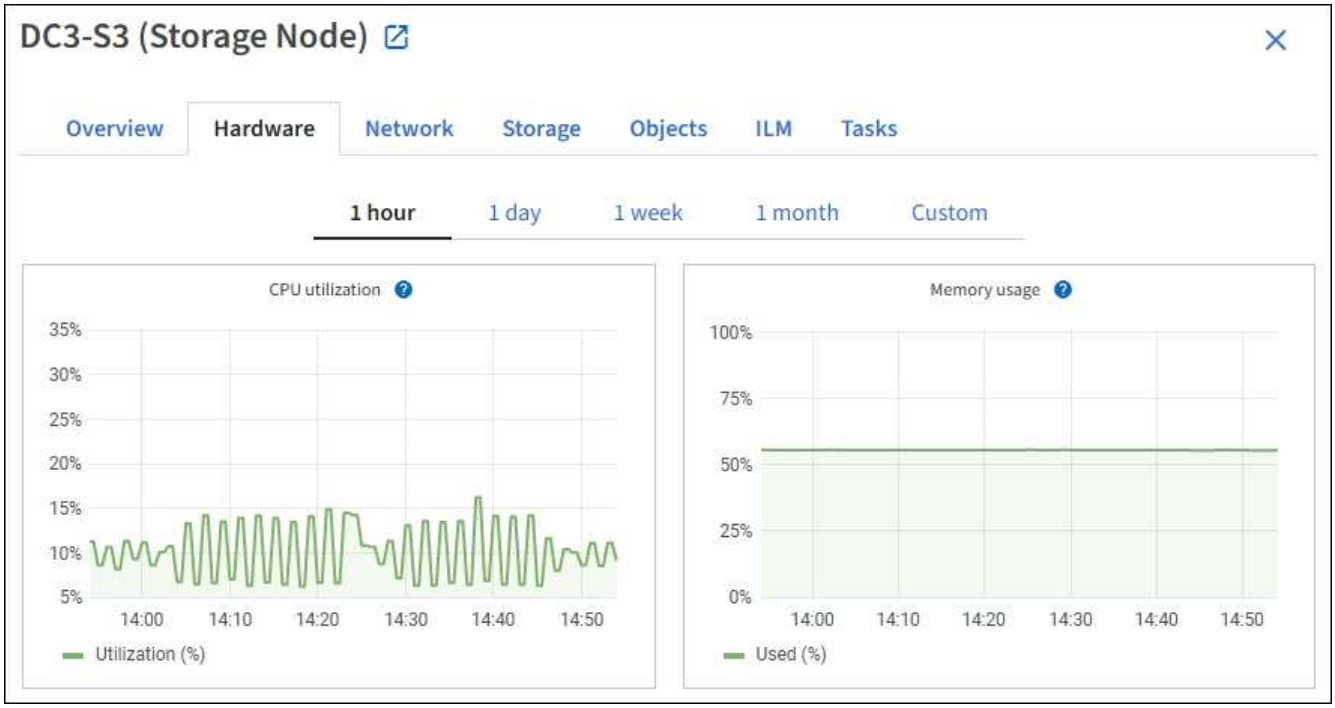
Antes de começar

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

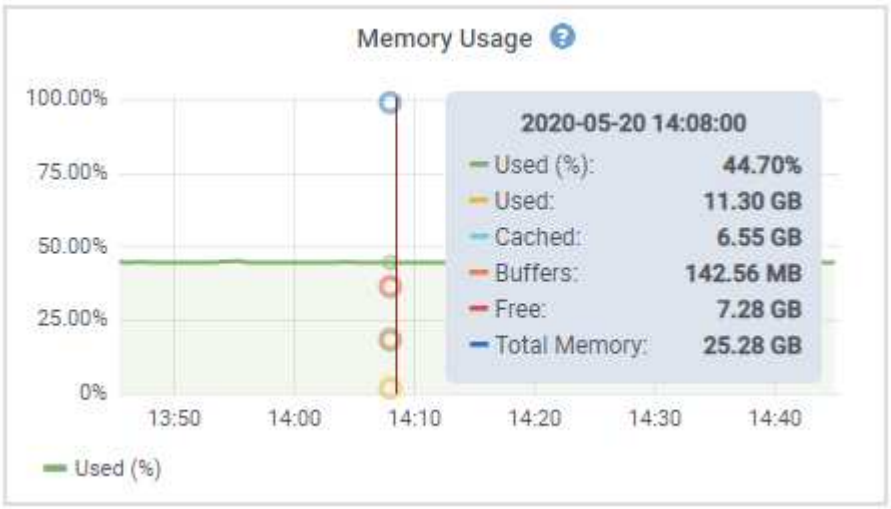
Passos

1. Selecione **NODES**. Em seguida, selecione um nó, um site ou a grade inteira.
2. Selecione a aba cujas informações você deseja visualizar.

Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas do Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **Hardware** para um nó inclui dois gráficos Grafana.



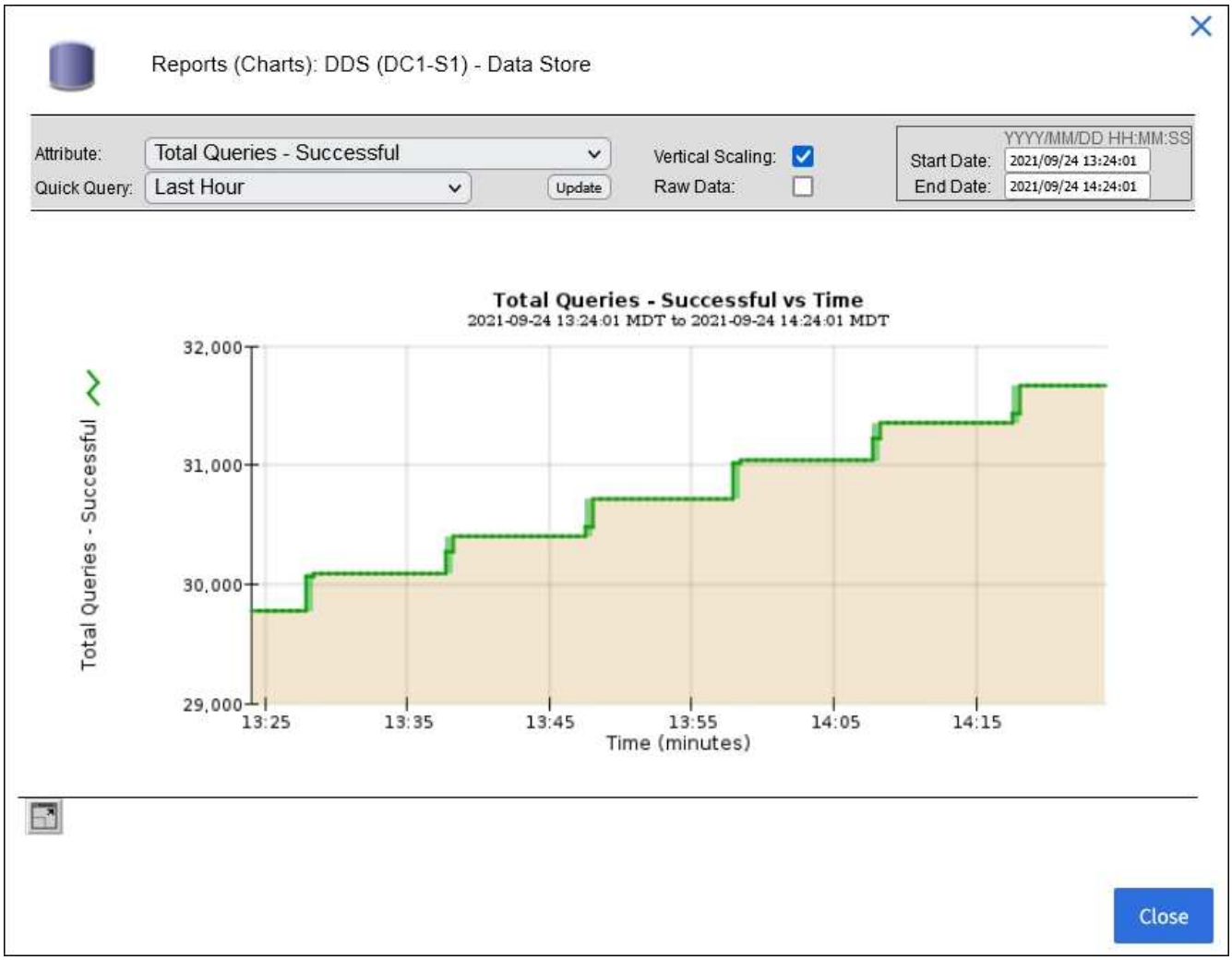
3. Opcionalmente, posicione o cursor sobre o gráfico para ver valores mais detalhados de um determinado momento.

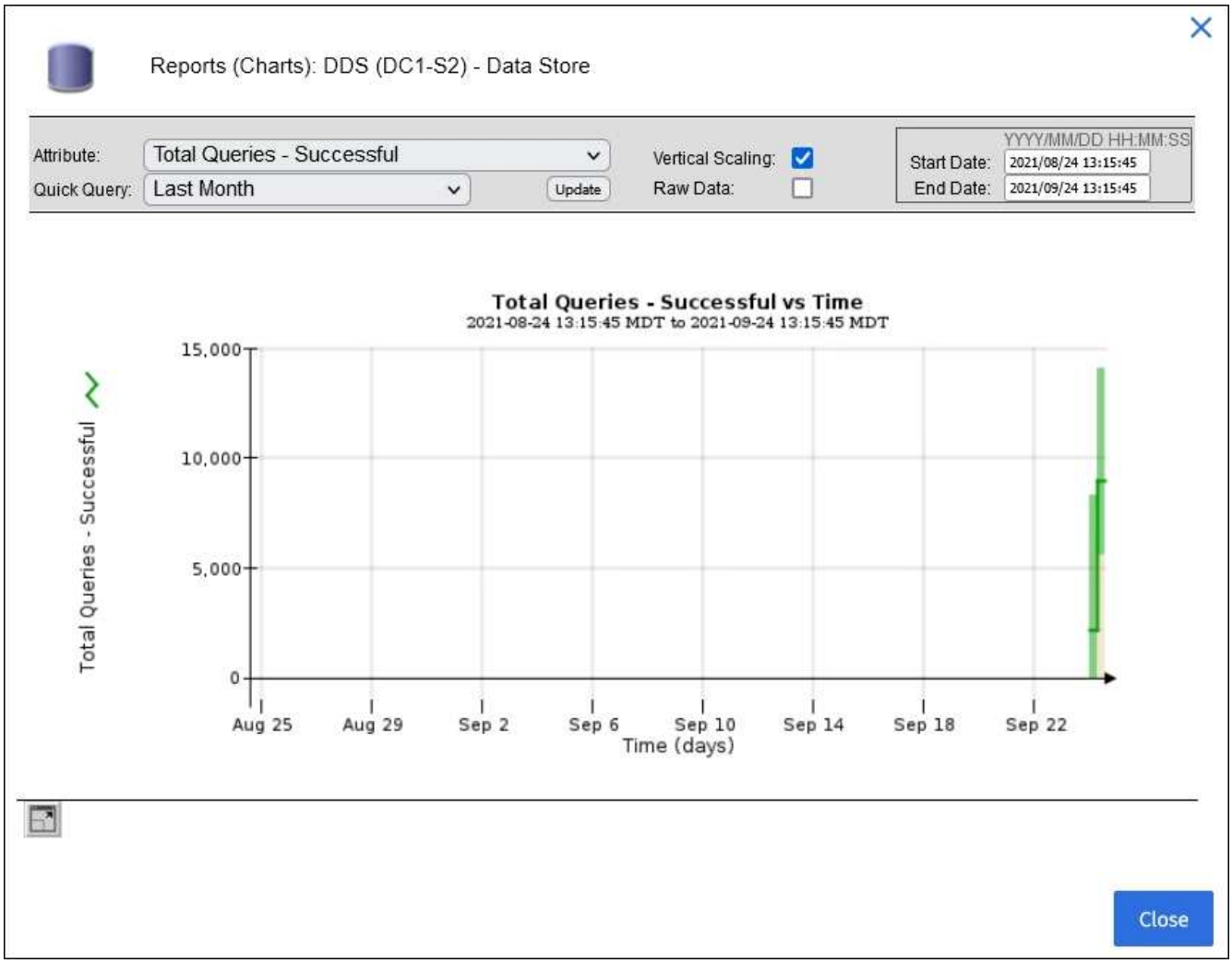


4. Conforme necessário, muitas vezes você pode exibir um gráfico para um atributo ou métrica específica. Na tabela na página Nós, selecione o ícone do gráfico à direita do nome do atributo.

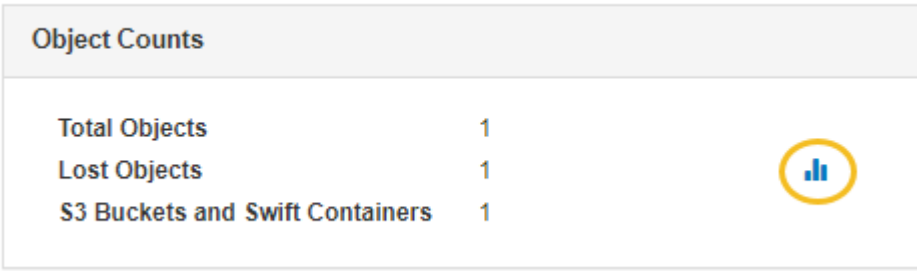
> Os gráficos não estão disponíveis para todas as métricas e atributos.

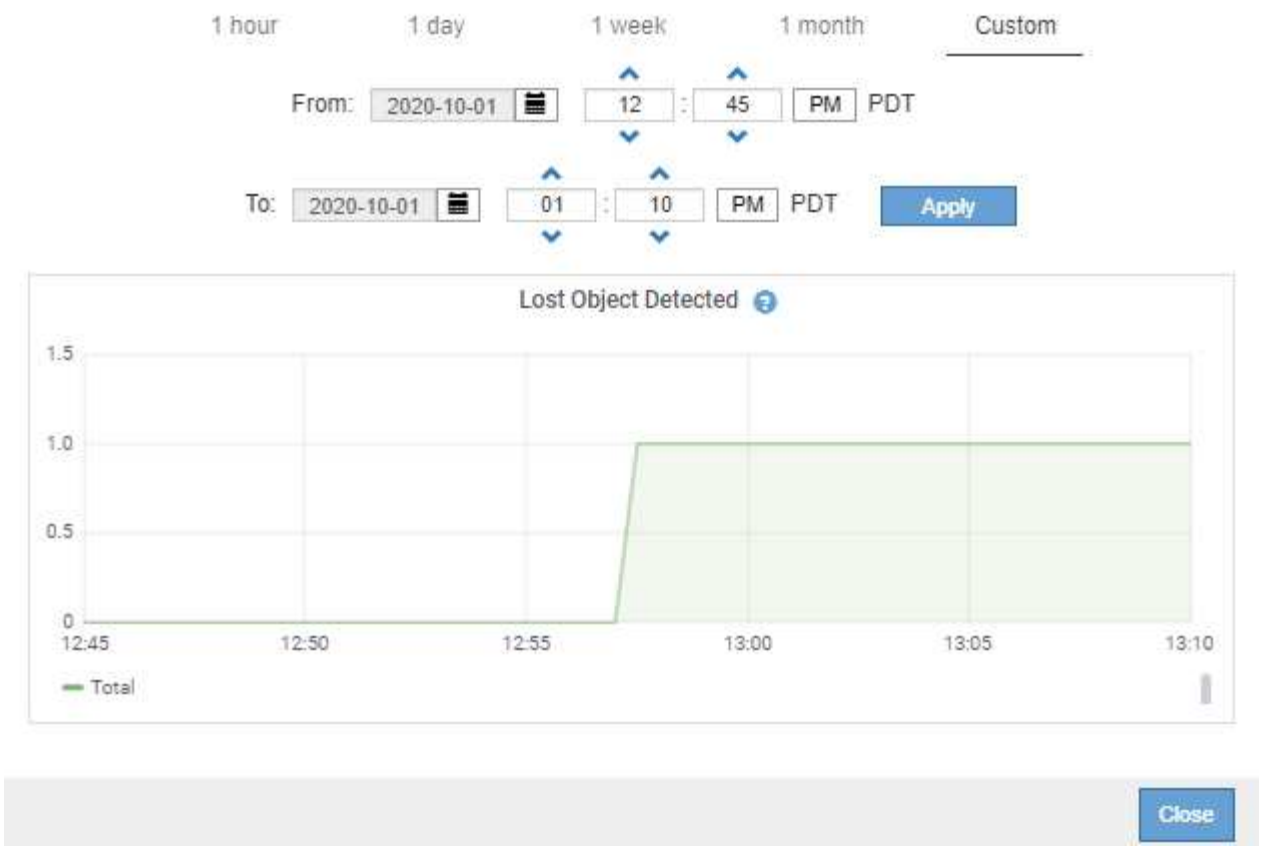
Exemplo 1: Na guia Objetos de um Nó de Armazenamento, você pode selecionar o ícone do gráfico para ver o número total de consultas bem-sucedidas do repositório de metadados para o nó de armazenamento.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

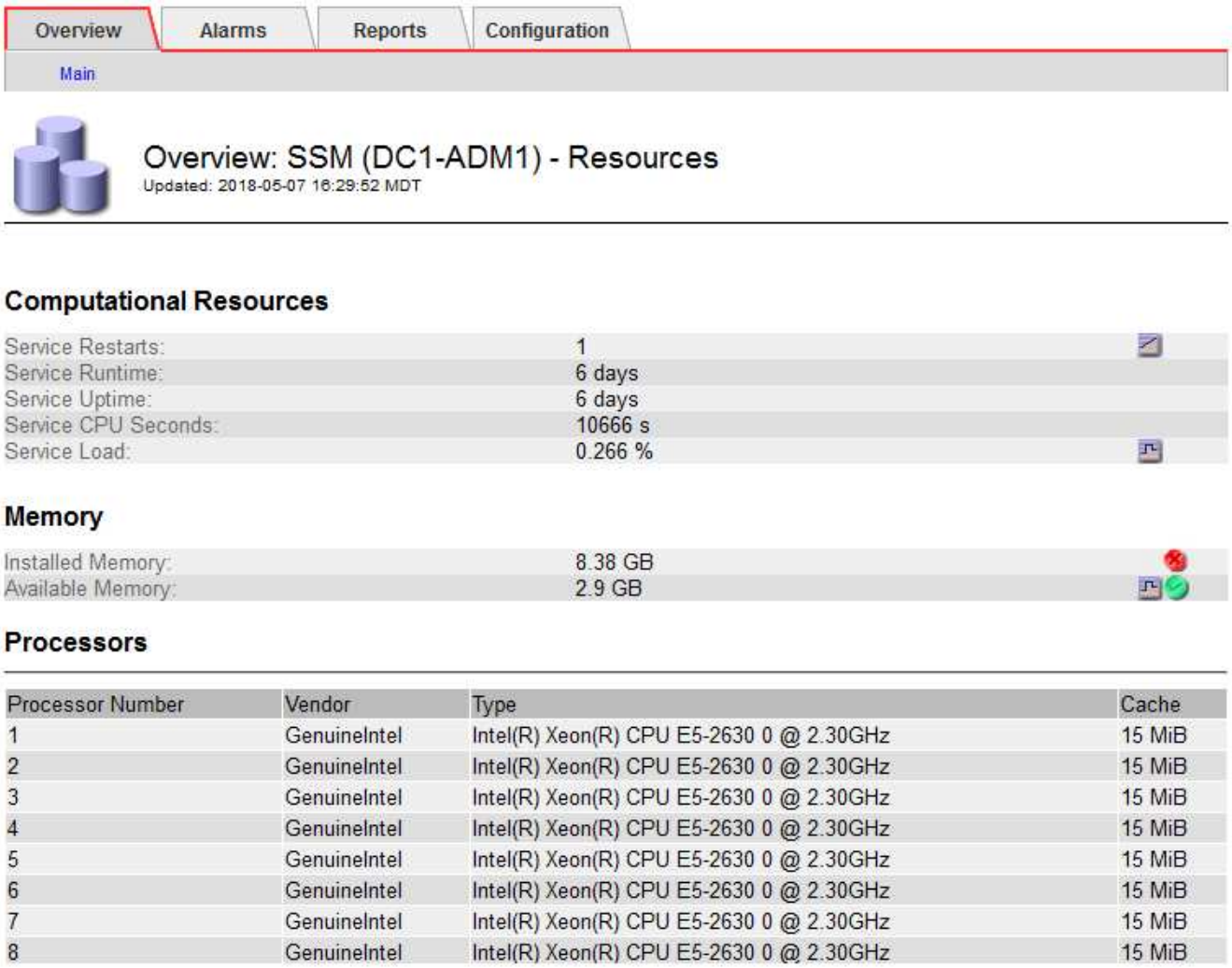


Exemplo 2: Na guia Objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o gráfico Grafana da contagem de objetos perdidos detectados ao longo do tempo.





5. Para exibir gráficos para atributos que não são mostrados na página Nó, selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
6. Selecione ***nó de grade*** > ***componente ou serviço*** > **Visão geral** > **Principal**.



7. Selecione o ícone do gráfico ao lado do atributo.

   A exibição muda automaticamente para a página **Relatórios** > **Gráficos**. O gráfico exibe os dados do atributo no último dia.

Gerar gráficos

Os gráficos exibem uma representação gráfica dos valores de dados de atributos. Você pode gerar relatórios sobre um site de data center, nó de grade, componente ou serviço.

Antes de começar

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

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***grid node*** > ***component or service*** > **Relatórios** > **Gráficos**.
3. Selecione o atributo a ser relatado na lista suspensa **Atributo**.
4. Para forçar o eixo Y a começar em zero, desmarque a caixa de seleção **Escala vertical**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **Dados Brutos** ou, para arredondar

os valores para um máximo de três casas decimais (por exemplo, para atributos relatados como porcentagens), desmarque a caixa de seleção **Dados Brutos**.

6. Selecione o período de tempo para relatar na lista suspensa **Consulta rápida**.

   Selecione a opção Consulta personalizada para selecionar um intervalo de tempo específico.

   O gráfico aparece depois de alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos.

7. Se você selecionou Consulta personalizada, personalize o período do gráfico inserindo a **Data de início** e a **Data de término**.

   Use o formato *YYYY/MM/DDHH:MM:SS* no horário local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Selecione **Atualizar**.

   Um gráfico é gerado após alguns segundos. Reserve vários minutos para tabulação de intervalos de tempo longos. Dependendo do período definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado será exibido.

Usar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Há dois tipos de relatórios gerados dependendo do período de tempo em que você está relatando: relatórios de texto bruto para períodos inferiores a uma semana e relatórios de texto agregado para períodos superiores a uma semana.

Relatórios de texto bruto

Um relatório de texto bruto exibe detalhes sobre o atributo selecionado:

- Hora de recebimento: data e hora locais em que um valor de amostra dos dados de um atributo foi processado pelo serviço NMS.
- Hora da amostra: data e hora locais em que um valor de atributo foi amostrado ou alterado na origem.
- Valor: Valor do atributo no momento da amostra.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Relatórios de texto agregado

Um relatório de texto agregado exibe dados durante um período de tempo mais longo (geralmente uma semana) do que um relatório de texto bruto. Cada entrada é o resultado do resumo de vários valores de atributos (um agregado de valores de atributos) pelo serviço NMS ao longo do tempo em uma única entrada com valores médios, máximos e mínimos derivados da agregação.

Cada entrada exibe as seguintes informações:

- Hora agregada: última data e hora local em que o serviço NMS agregou (coletou) um conjunto de valores de atributos alterados.
- Valor médio: a média do valor do atributo ao longo do período de tempo agregado.
- Valor mínimo: o valor mínimo ao longo do período de tempo agregado.
- Valor máximo: o valor máximo durante o período de tempo agregado.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Gerar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Você pode gerar relatórios sobre um site de data center, nó de grade, componente ou serviço.

Antes de começar

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

Sobre esta tarefa

Para dados de atributos que devem mudar continuamente, esses dados de atributos são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributo que mudam com pouca frequência (por exemplo, dados baseados em eventos como alterações de estado ou status), um valor de atributo é enviado ao serviço NMS quando o valor muda.

O tipo de relatório exibido depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos maiores que uma semana.

O texto em cinza indica que o serviço estava administrativamente inativo durante o período em que foi amostrado. O texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***nó de grade*** > ***componente ou serviço*** > **Relatórios** > **Texto**.
3. Selecione o atributo a ser relatado na lista suspensa **Atributo**.
4. Selecione o número de resultados por página na lista suspensa **Resultados por página**.
5. Para arredondar valores para um máximo de três casas decimais (por exemplo, para atributos relatados como porcentagens), desmarque a caixa de seleção **Dados Brutos**.
6. Selecione o período de tempo para relatar na lista suspensa **Consulta rápida**.

   Selecione a opção Consulta personalizada para selecionar um intervalo de tempo específico.

O relatório aparece depois de alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos.

7. Se você selecionou Consulta personalizada, precisará personalizar o período de tempo do relatório inserindo a **Data de início** e a **Data de término**.

   Use o formato `YYYY/MM/DDHH:MM:SS` no horário local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Clique em **Atualizar**.

   Um relatório de texto é gerado após alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos. Dependendo do período definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado será exibido.

Exportar relatórios de texto

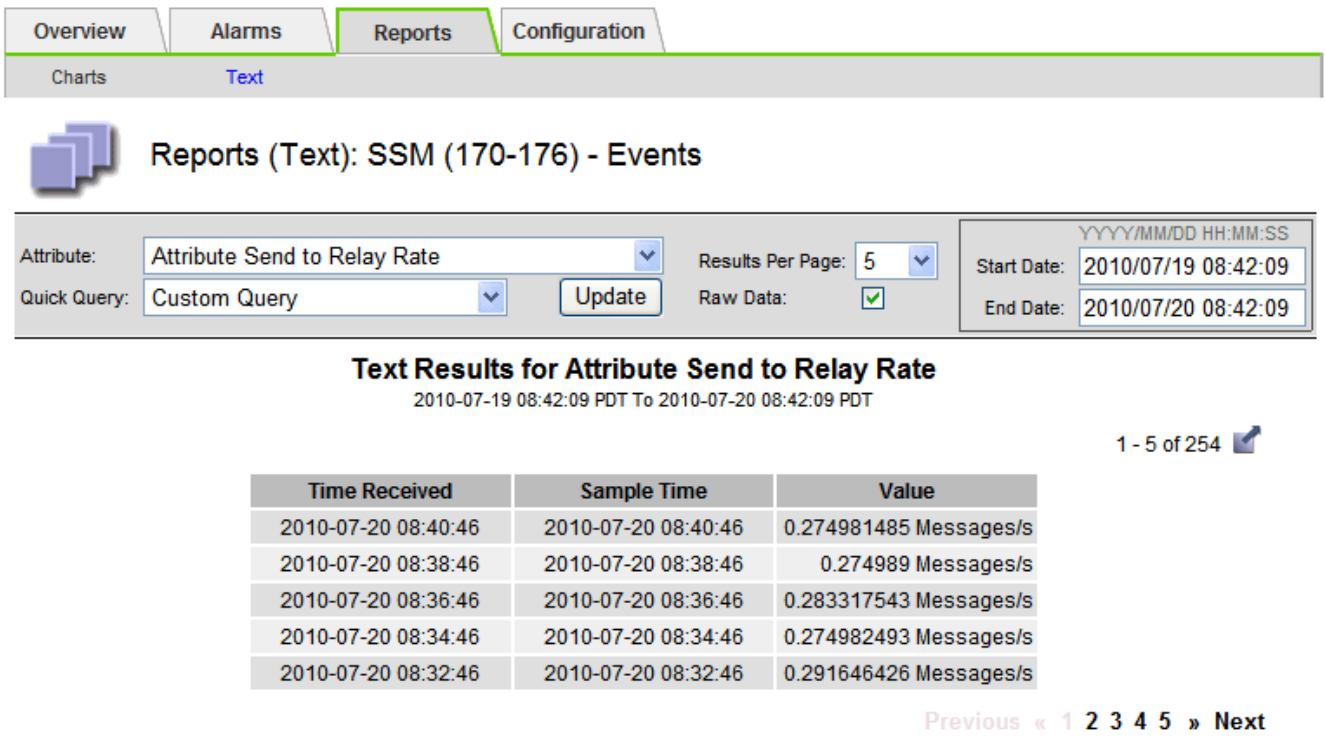
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

Sobre esta tarefa

Os dados copiados podem então ser salvos em um novo documento (por exemplo, uma planilha) e usados para analisar o desempenho do sistema StorageGRID .

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Crie um relatório de texto.
3. Clique em *Exportar* .



A janela Exportar Relatório de Texto é aberta exibindo o relatório.

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Selecione e copie o conteúdo da janela Exportar Relatório de Texto.

   Esses dados agora podem ser colados em um documento de terceiros, como uma planilha.

Monitore o desempenho de PUT e GET

Você pode monitorar o desempenho de determinadas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir investigação adicional.

Sobre esta tarefa

Para monitorar o desempenho de PUT e GET, você pode executar comandos S3 diretamente de uma estação de trabalho ou usando o aplicativo S3tester de código aberto. O uso desses métodos permite avaliar o desempenho independentemente de fatores externos ao StorageGRID, como problemas com um aplicativo cliente ou problemas com uma rede externa.

Ao executar testes de operações PUT e GET, use as seguintes diretrizes:

- Use tamanhos de objetos comparáveis aos objetos que você normalmente ingere em sua grade.
- Execute operações em sites locais e remotos.

Mensagens no"registro de auditoria" indicar o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação S3 GET, você pode revisar o valor do atributo TIME na mensagem de auditoria SGET. Você também pode encontrar o atributo TIME nas mensagens de auditoria para as seguintes operações do S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o rendimento geral que você pode atingir. Repita os mesmos testes regularmente e registre os resultados para que você possa identificar tendências que possam exigir investigação.

- Você pode "baixe o S3tester do github" .

Monitorar operações de verificação de objetos

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .

Sobre esta tarefa

Dois"processos de verificação" trabalhar em conjunto para garantir a integridade dos dados:

- **A verificação de antecedentes** é executada automaticamente, verificando continuamente a exatidão dos dados do objeto.

  A verificação em segundo plano verifica automática e continuamente todos os nós de armazenamento para determinar se há cópias corrompidas de dados de objetos replicados e codificados para eliminação. Se forem encontrados problemas, o sistema StorageGRID tenta automaticamente substituir os dados do objeto corrompidos de cópias armazenadas em outro lugar no sistema. A verificação em segundo plano não é executada em objetos em um pool de armazenamento em nuvem.

  > ⓘ O alerta **Objeto corrompido não identificado detectado** é acionado se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente.

- **A verificação de existência de objetos** pode ser acionada por um usuário para verificar mais rapidamente a existência (mas não a exatidão) dos dados do objeto.

  A verificação de existência de objetos verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados para eliminação existem em um nó de armazenamento. A verificação de existência de objetos fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware pode ter afetado a integridade dos dados.

Você deve revisar os resultados das verificações de antecedentes e verificações de existência de objetos regularmente. Investigue imediatamente quaisquer instâncias de dados de objetos corrompidos ou ausentes para determinar a causa raiz.

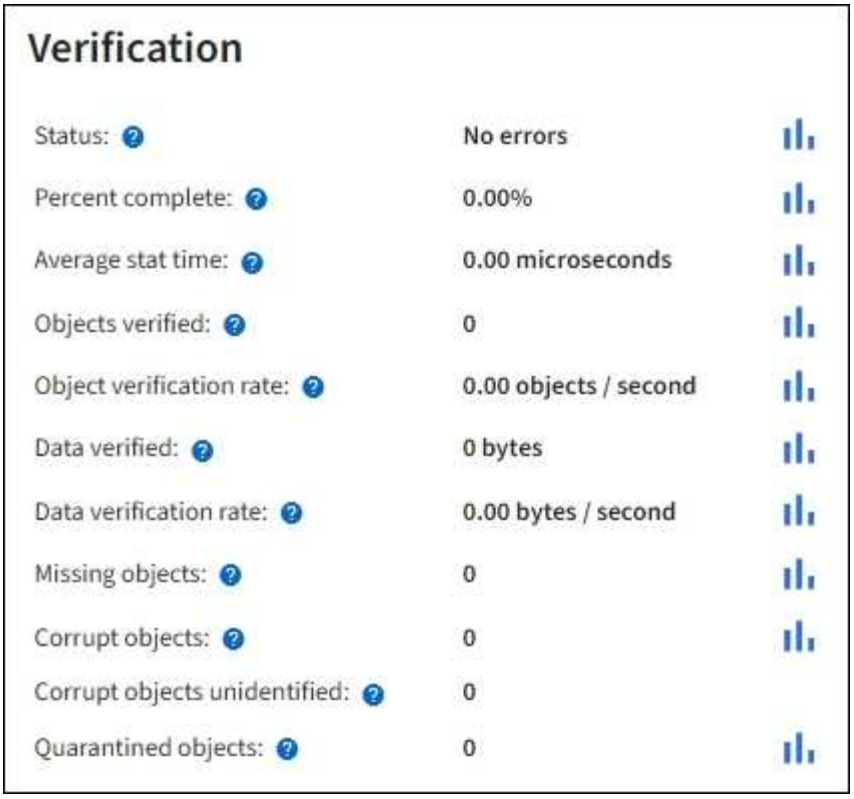
Passos

1. Revise os resultados das verificações de antecedentes:

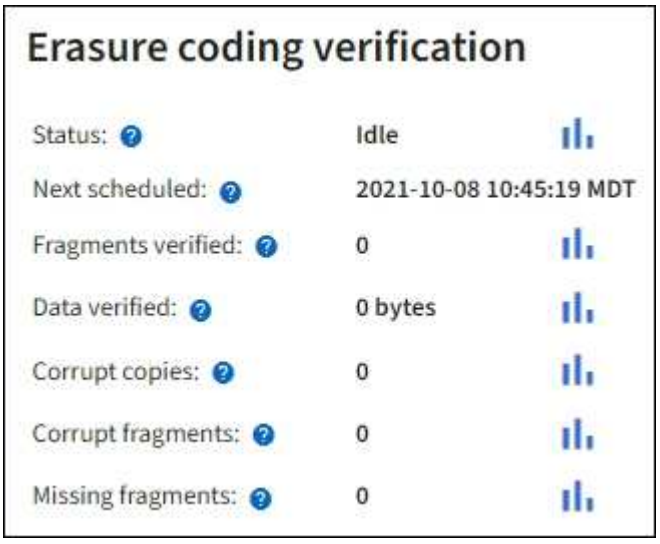
   a. Selecione **NÓS** > ***Nó de Armazenamento*** > **Objetos**.

   b. Confira os resultados da verificação:

      - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.

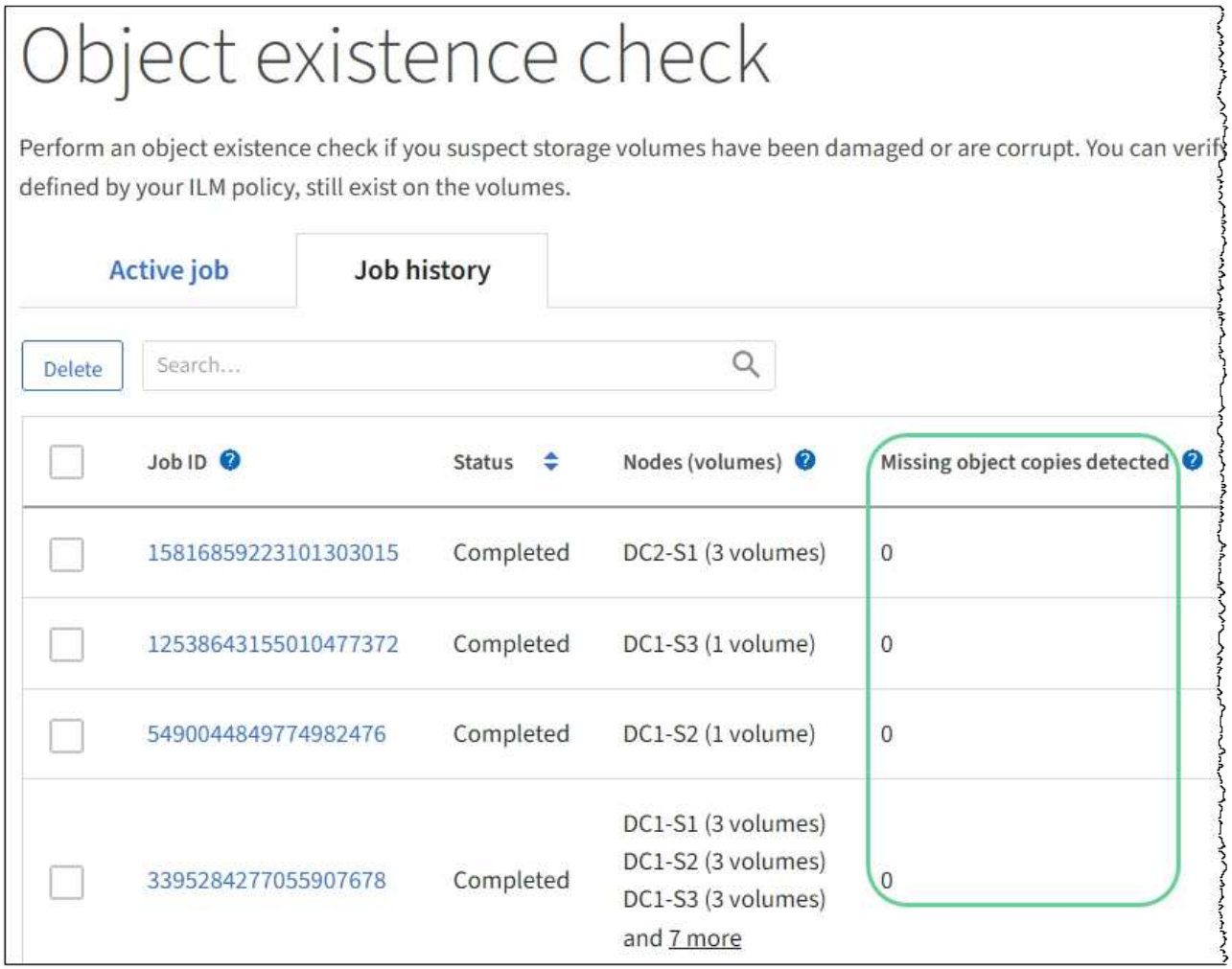


- Para verificar a verificação de fragmentos codificados por eliminação, selecione ***Storage Node*** > **ILM** e observe os atributos na seção Verificação de codificação de eliminação.



Selecione o ponto de interrogação ao lado do nome de um atributo para exibir o texto de ajuda.

2. Revise os resultados dos trabalhos de verificação de existência de objetos:
   a. Selecione **MANUTENÇÃO** > **Verificação de existência do objeto** > **Histórico de tarefas**.
   b. Examine a coluna Cópias de objetos ausentes detectadas. Se algum trabalho resultou em 100 ou mais cópias de objetos ausentes e o alerta **Objetos perdidos** foi acionado, entre em contato com o suporte técnico.



Monitorar eventos

Você pode monitorar eventos detectados por um nó de grade, incluindo eventos personalizados que você criou para rastrear eventos registrados no servidor syslog. A mensagem Último Evento exibida no Grid Manager fornece mais informações sobre o evento mais recente.

As mensagens de eventos também são listadas no `/var/local/log/bycast-err.log` arquivo de log. Veja o"Referência de arquivos de log" .

O alarme SMTT (Total de eventos) pode ser disparado repetidamente por problemas como problemas de rede, quedas de energia ou atualizações. Esta seção contém informações sobre como investigar eventos para que você possa entender melhor por que esses alarmes ocorreram. Se um evento ocorreu devido a um problema conhecido, é seguro redefinir os contadores de eventos.

Passos

1. Revise os eventos do sistema para cada nó da grade:
   a. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
   b. Selecione ***site*** > ***grid node*** > **SSM** > **Eventos** > **Visão geral** > **Principal**.
2. Gere uma lista de mensagens de eventos anteriores para ajudar a isolar problemas que ocorreram no passado:

a. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.

b. Selecione ***site*** > ***grid node*** > **SSM** > **Eventos** > **Relatórios**.

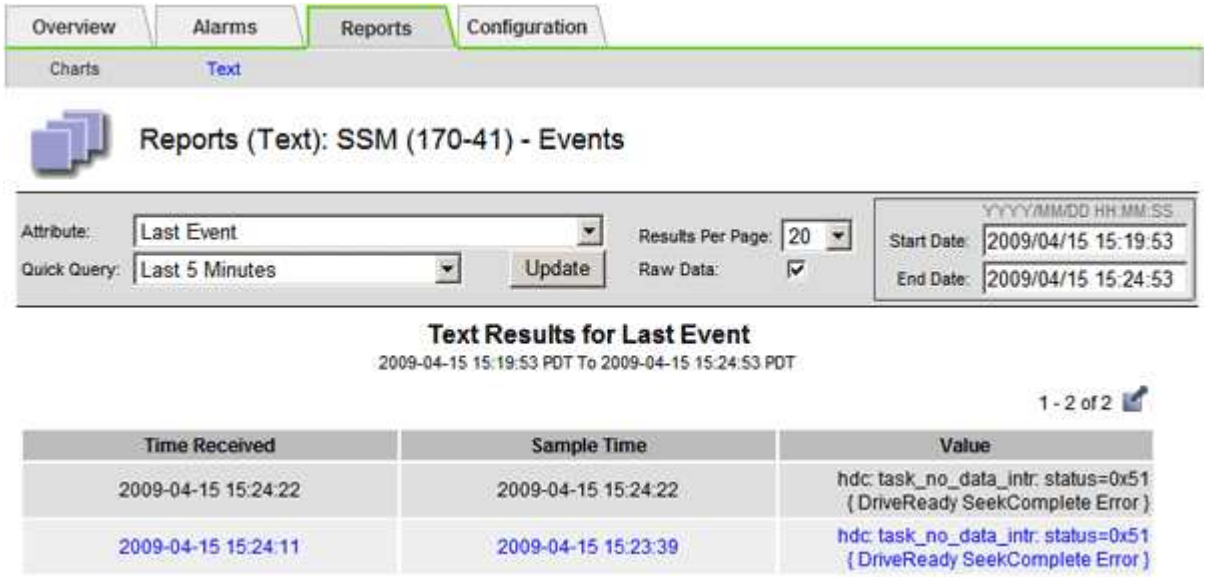
c. Selecione **Texto**.

O atributo **Último Evento** não é mostrado no"visualização de gráficos" . Para visualizá-lo:

d. Altere **Atributo** para **Último Evento**.

e. Opcionalmente, selecione um período de tempo para **Consulta rápida**.

f. Selecione **Atualizar**.



Criar eventos syslog personalizados

Eventos personalizados permitem que você rastreie todos os eventos de kernel, daemon, erro e nível crítico do usuário registrados no servidor syslog. Um evento personalizado pode ser útil para monitorar a ocorrência de mensagens de log do sistema (e, portanto, eventos de segurança de rede e falhas de hardware).

Sobre esta tarefa

Considere criar eventos personalizados para monitorar problemas recorrentes. As considerações a seguir se aplicam a eventos personalizados.

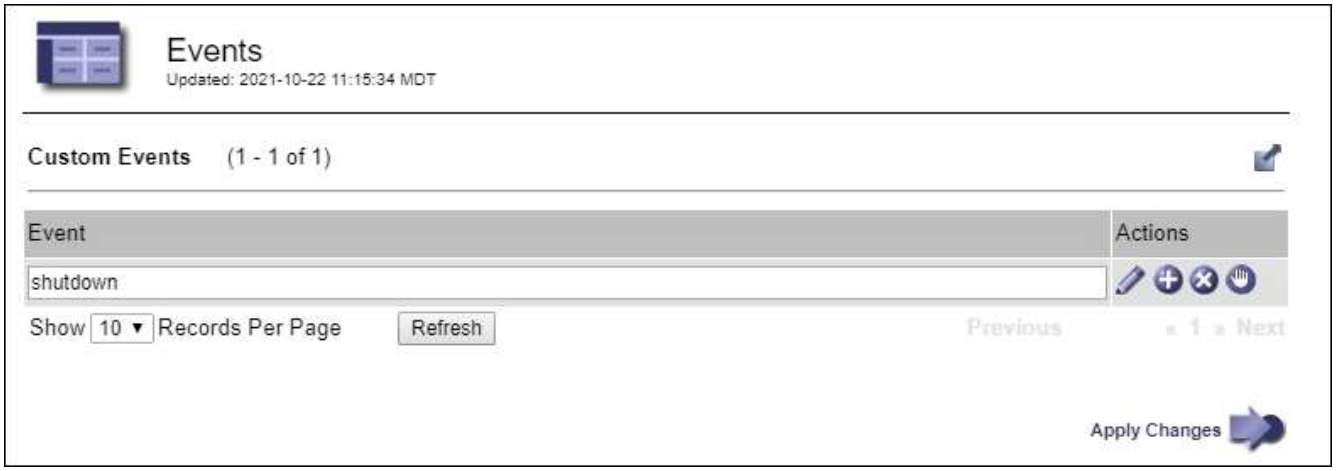
- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada.
- Para criar um evento personalizado com base em palavras-chave no `/var/local/log/messages` arquivos, os logs nesses arquivos devem ser:
  - Gerado pelo kernel
  - Gerado pelo daemon ou programa do usuário no nível de erro ou crítico

Nota: Nem todas as entradas no `/var/local/log/messages` os arquivos serão correspondidos, a menos que satisfaçam os requisitos declarados acima.

Passos

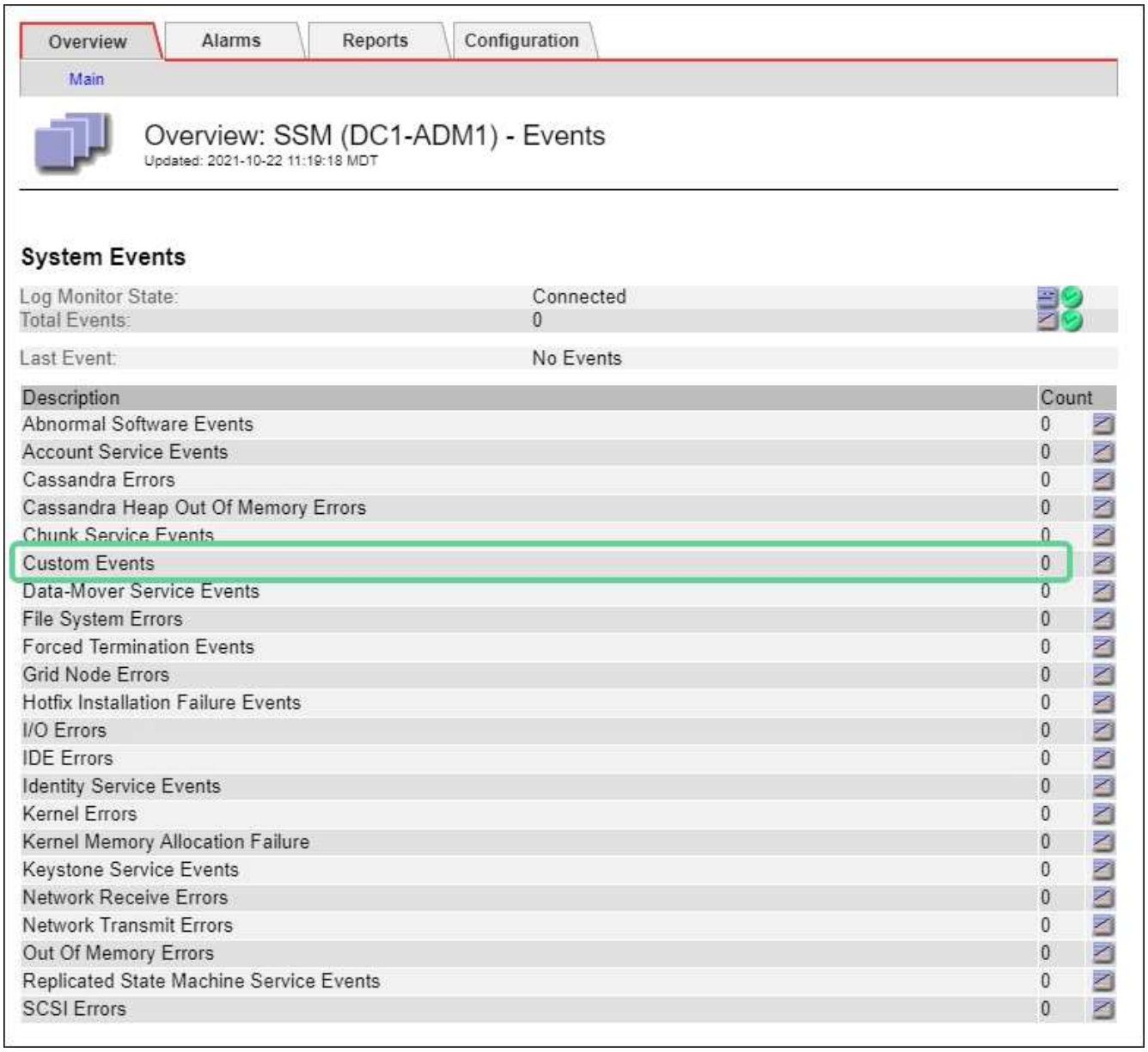
1. Selecione **SUPORTE** > **Alarmes (antigo)** > **Eventos personalizados**.
2. Clique em *Editar* (ou *Inserir* se este não for o primeiro evento).

3. Insira uma sequência de eventos personalizada, por exemplo, desligamento



4. Selecione **Aplicar alterações**.
5. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
6. Selecione ***grid node*** > **SSM** > **Eventos**.
7. Localize a entrada para Eventos personalizados na tabela Eventos e monitore o valor para **Contagem**.

   Se a contagem aumentar, um evento personalizado que você está monitorando será acionado naquele nó da grade.



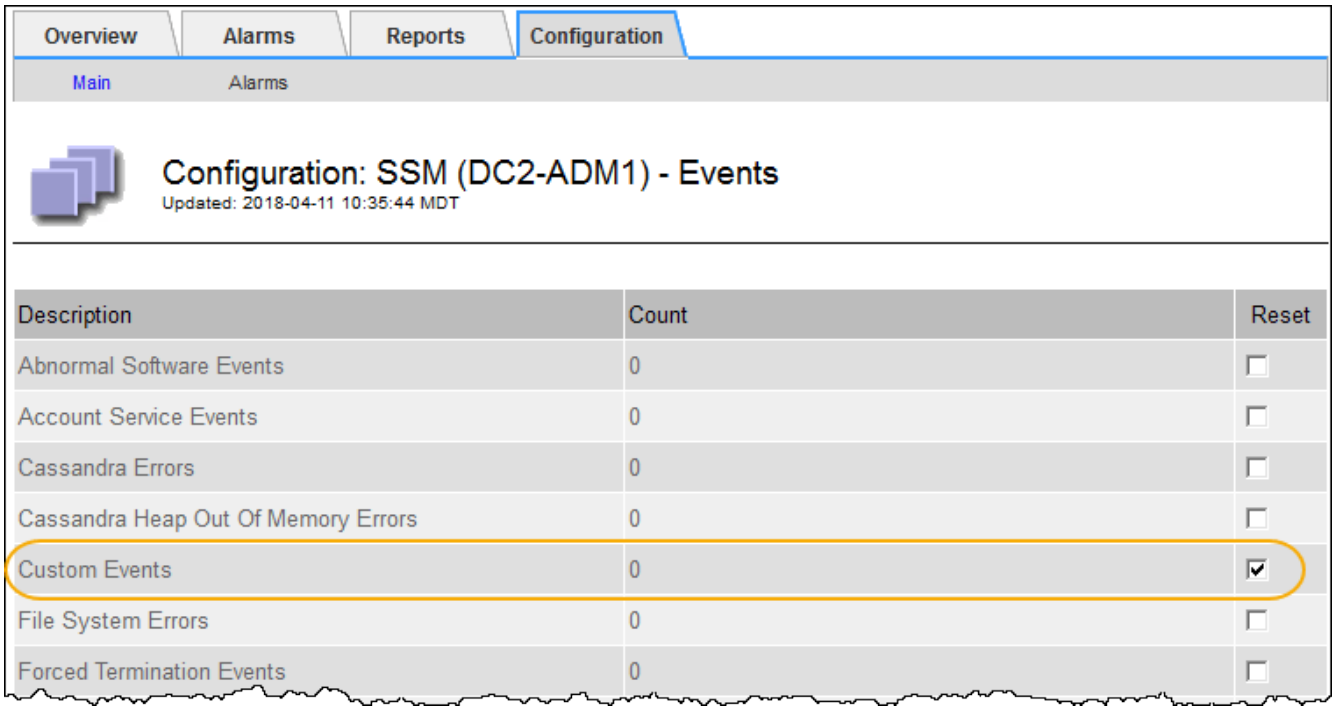
Redefina a contagem de eventos personalizados para zero

Se você quiser zerar o contador apenas para eventos personalizados, use a página Topologia de grade no menu Suporte.

Redefinir um contador faz com que o alarme seja disparado pelo próximo evento. Por outro lado, quando você reconhece um alarme, ele só é disparado novamente se o próximo nível limite for atingido.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***grid node*** > **SSM** > **Eventos** > **Configuração** > **Principal**.
3. Selecione a caixa de seleção **Redefinir** para Eventos personalizados.



4. Selecione **Aplicar alterações**.

Revisar mensagens de auditoria

As mensagens de auditoria podem ajudar você a entender melhor as operações detalhadas do seu sistema StorageGRID . Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços do StorageGRID geram mensagens de auditoria, como a seguir:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de armazenamento de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento e recuperações de objetos, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento registram solicitações do usuário para a API de gerenciamento.

Cada nó de administração armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compactados de dias anteriores. Cada nó na grade também armazena uma cópia das informações de auditoria geradas no nó.

Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó de administração.

O StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- O StorageGRID assume como padrão os destinos de auditoria de nós locais.
- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de

armazenamento.

- Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado.
- "Saiba mais sobre como configurar mensagens de auditoria e destinos de log" .

Para obter detalhes sobre o arquivo de log de auditoria, o formato das mensagens de auditoria, os tipos de mensagens de auditoria e as ferramentas disponíveis para analisar mensagens de auditoria, consulte"Revisar logs de auditoria" .

Coletar arquivos de log e dados do sistema

Você pode usar o Grid Manager para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID .

Antes de começar

- Você deve estar conectado ao Grid Manager no nó de administração primário usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você deve ter a senha de provisionamento.

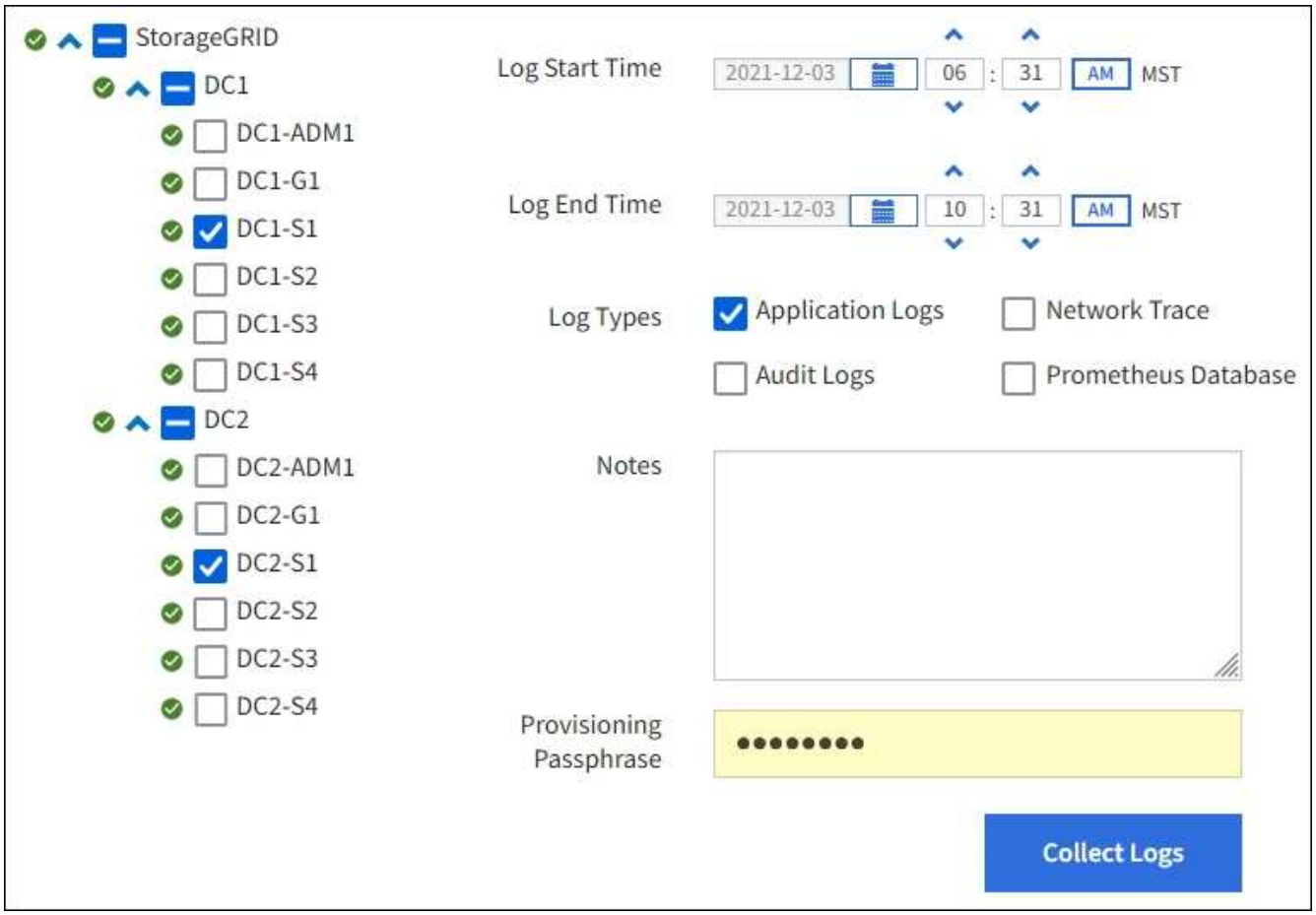
Sobre esta tarefa

Você pode usar o Grid Manager para reunir"arquivos de log" , dados do sistema e dados de configuração de qualquer nó de grade para o período de tempo selecionado. Os dados são coletados e arquivados em um arquivo .tar.gz que você pode baixar para seu computador local.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver "Configurar mensagens de auditoria e destinos de log" .

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Registros**.



2. Selecione os nós da grade para os quais você deseja coletar arquivos de log.

   Conforme necessário, você pode coletar arquivos de log para toda a grade ou para um site de data center inteiro.

3. Selecione uma **Hora de início** e uma **Hora de término** para definir o intervalo de tempo dos dados a serem incluídos nos arquivos de log.

   Se você selecionar um período de tempo muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de log poderá ficar muito grande para ser armazenado em um nó ou muito grande para ser coletado no nó de administração principal para download. Se isso ocorrer, você deverá reiniciar a coleta de logs com um conjunto menor de dados.

4. Selecione os tipos de logs que você deseja coletar.
   - **Logs de aplicativos**: logs específicos do aplicativo que o suporte técnico usa com mais frequência para solução de problemas. Os logs coletados são um subconjunto dos logs de aplicativos disponíveis.
   - **Registros de auditoria**: Registros contendo as mensagens de auditoria geradas durante a operação normal do sistema.
   - **Rastreamento de rede**: Logs usados para depuração de rede.
   - **Banco de dados Prometheus**: métricas de séries temporais dos serviços em todos os nós.
5. Opcionalmente, insira notas sobre os arquivos de log que você está coletando na caixa de texto **Notas**.

   Você pode usar essas notas para fornecer informações de suporte técnico sobre o problema que o levou a coletar os arquivos de log. Suas notas são adicionadas a um arquivo chamado `info.txt` , juntamente com outras informações sobre a coleção de arquivos de log. O `info.txt` o arquivo é salvo no pacote de

arquivo de log.

6. Digite a senha de provisionamento do seu sistema StorageGRID na caixa de texto **Senha de provisionamento**.
7. Selecione **Coletar Logs**.

   Quando você envia uma nova solicitação, a coleção anterior de arquivos de log é excluída.

   Você pode usar a página Logs para monitorar o progresso da coleta de arquivos de log para cada nó da grade.

   Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo mais curto ou para menos nós.

8. Selecione **Download** quando a coleta do arquivo de log estiver concluída.

   O arquivo *.tar.gz* contém todos os arquivos de log de todos os nós da grade onde a coleta de log foi bem-sucedida. Dentro do arquivo combinado *.tar.gz*, há um arquivo de log para cada nó da grade.

Depois que você terminar

Você pode baixar novamente o pacote de arquivo de log mais tarde, se necessário.

Opcionalmente, você pode selecionar **Excluir** para remover o pacote de arquivamento do arquivo de log e liberar espaço em disco. O pacote de arquivo de log atual será removido automaticamente na próxima vez que você coletar arquivos de log.

Acionar manualmente um pacote AutoSupport

Para auxiliar o suporte técnico na solução de problemas com seu sistema StorageGRID , você pode acionar manualmente o envio de um pacote AutoSupport .

Antes de começar

- Você deve estar conectado ao Grid Manager usando um"navegador da web compatível" .
- Você deve ter acesso Root ou permissão para Outra configuração de grade.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport*.
2. Na guia **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar um pacote de AutoSupport para o site de suporte da NetApp . Se a tentativa for bem-sucedida, os valores **Resultado mais recente** e **Última hora bem-sucedida** na guia **Resultados** serão atualizados. Se houver um problema, o valor **Resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.

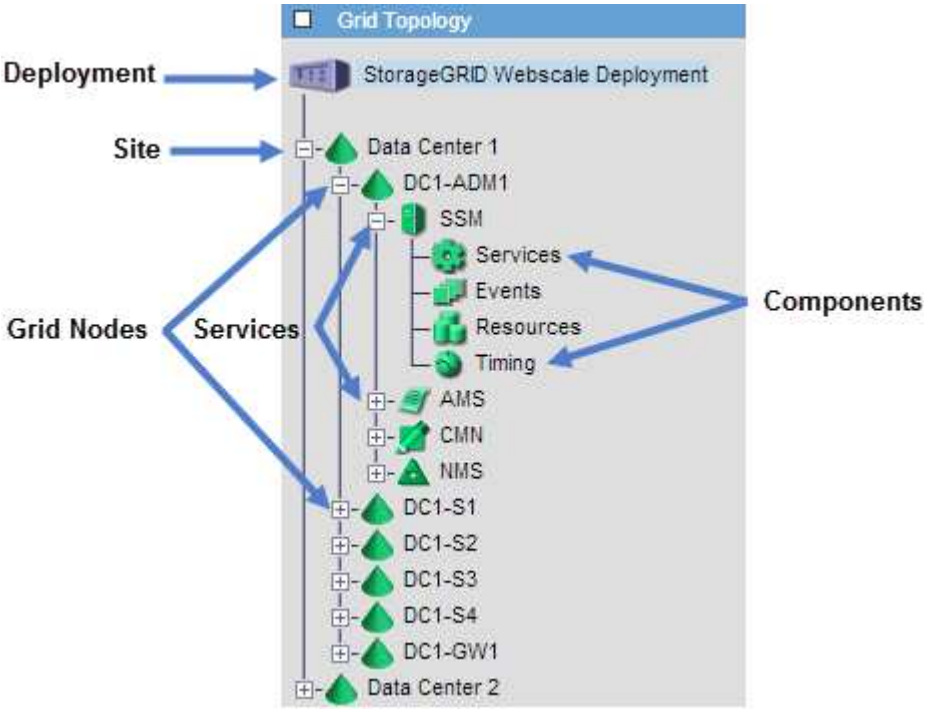
   Após enviar um pacote de AutoSupport acionado pelo usuário, atualize a página de AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Visualizar a árvore de topologia da grade

A árvore de topologia de grade fornece acesso a informações detalhadas sobre os elementos do sistema StorageGRID , incluindo sites, nós de grade, serviços e

componentes. Na maioria dos casos, você só precisa acessar a árvore de topologia de grade quando instruído na documentação ou ao trabalhar com o suporte técnico.

Para acessar a árvore Topologia de grade, selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.



Para expandir ou recolher a árvore de topologia de grade, clique em ⊞ ou ⊟ no nível do site, nó ou serviço. Para expandir ou recolher todos os itens em todo o site ou em cada nó, mantenha pressionada a tecla **<Ctrl>** e clique.

Atributos StorageGRID

Os atributos relatam valores e status para muitas das funções do sistema StorageGRID . Os valores de atributo estão disponíveis para cada nó da grade, cada site e toda a grade.

Os atributos StorageGRID são usados em vários lugares no Grid Manager:

- **Página Nós**: Muitos dos valores mostrados na página Nós são atributos do StorageGRID . (As métricas do Prometheus também são mostradas nas páginas de nós.)
- **Árvore de topologia de grade**: os valores dos atributos são mostrados na árvore de topologia de grade (**SUPORTE** > **Ferramentas** > **Topologia de grade**).
- **Eventos**: Eventos do sistema ocorrem quando determinados atributos registram um erro ou condição de falha para um nó, incluindo erros como erros de rede.

Valores de atributos

Os atributos são relatados com base no melhor esforço e estão aproximadamente corretos. As atualizações de atributos podem ser perdidas em algumas circunstâncias, como a falha de um serviço ou a falha e reconstrução de um nó de grade.

Além disso, atrasos de propagação podem retardar o relato de atributos. Os valores atualizados para a maioria dos atributos são enviados ao sistema StorageGRID em intervalos fixos. Pode levar vários minutos até que uma atualização fique visível no sistema, e dois atributos que mudam mais ou menos

simultaneamente podem ser relatados em momentos ligeiramente diferentes.

Revisar métricas de suporte

Ao solucionar um problema, você pode trabalhar com o suporte técnico para revisar métricas e gráficos detalhados do seu sistema StorageGRID .

Antes de começar

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

Sobre esta tarefa

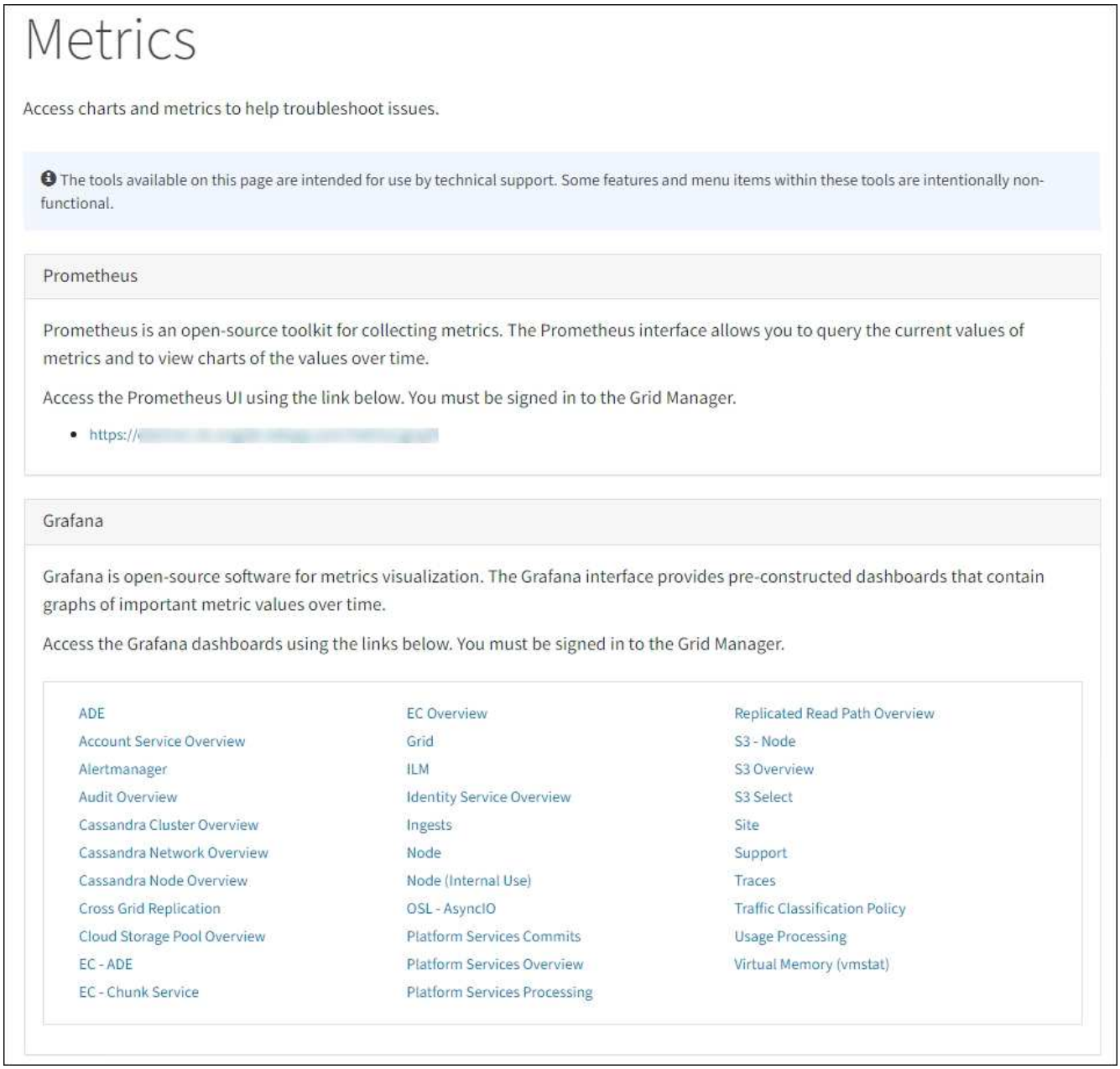
A página Métricas permite que você acesse as interfaces de usuário do Prometheus e do Grafana. Prometheus é um software de código aberto para coleta de métricas. Grafana é um software de código aberto para visualização de métricas.

> As ferramentas disponíveis na página Métricas são destinadas ao uso do suporte técnico. Alguns recursos e itens de menu dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Veja a lista de"métricas Prometheus comumente usadas" .

Passos

1. Conforme instruído pelo suporte técnico, selecione **SUPORTE** > **Ferramentas** > **Métricas**.

   Um exemplo da página Métricas é mostrado aqui:



2. Para consultar os valores atuais das métricas do StorageGRID e visualizar gráficos dos valores ao longo do tempo, clique no link na seção Prometheus.

   A interface do Prometheus é exibida. Você pode usar esta interface para executar consultas nas métricas do StorageGRID disponíveis e criar gráficos das métricas do StorageGRID ao longo do tempo.

   > Métricas que incluem *private* em seus nomes são destinadas apenas para uso interno e estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

3. Para acessar painéis pré-construídos contendo gráficos de métricas do StorageGRID ao longo do tempo, clique nos links na seção Grafana.

   A interface do Grafana para o link selecionado é exibida.

Executar diagnósticos

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no seu sistema StorageGRID e revisar os resultados.

- "Revisar métricas de suporte"
- "Métricas do Prometheus comumente usadas"

Antes de começar

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

Sobre esta tarefa

A página Diagnóstico executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um dos três status:

-

- **Normal**: Todos os valores estão dentro da faixa normal.
- **Atenção**: Um ou mais valores estão fora da faixa normal.
- **Cuidado**: Um ou mais valores estão significativamente fora da faixa normal.

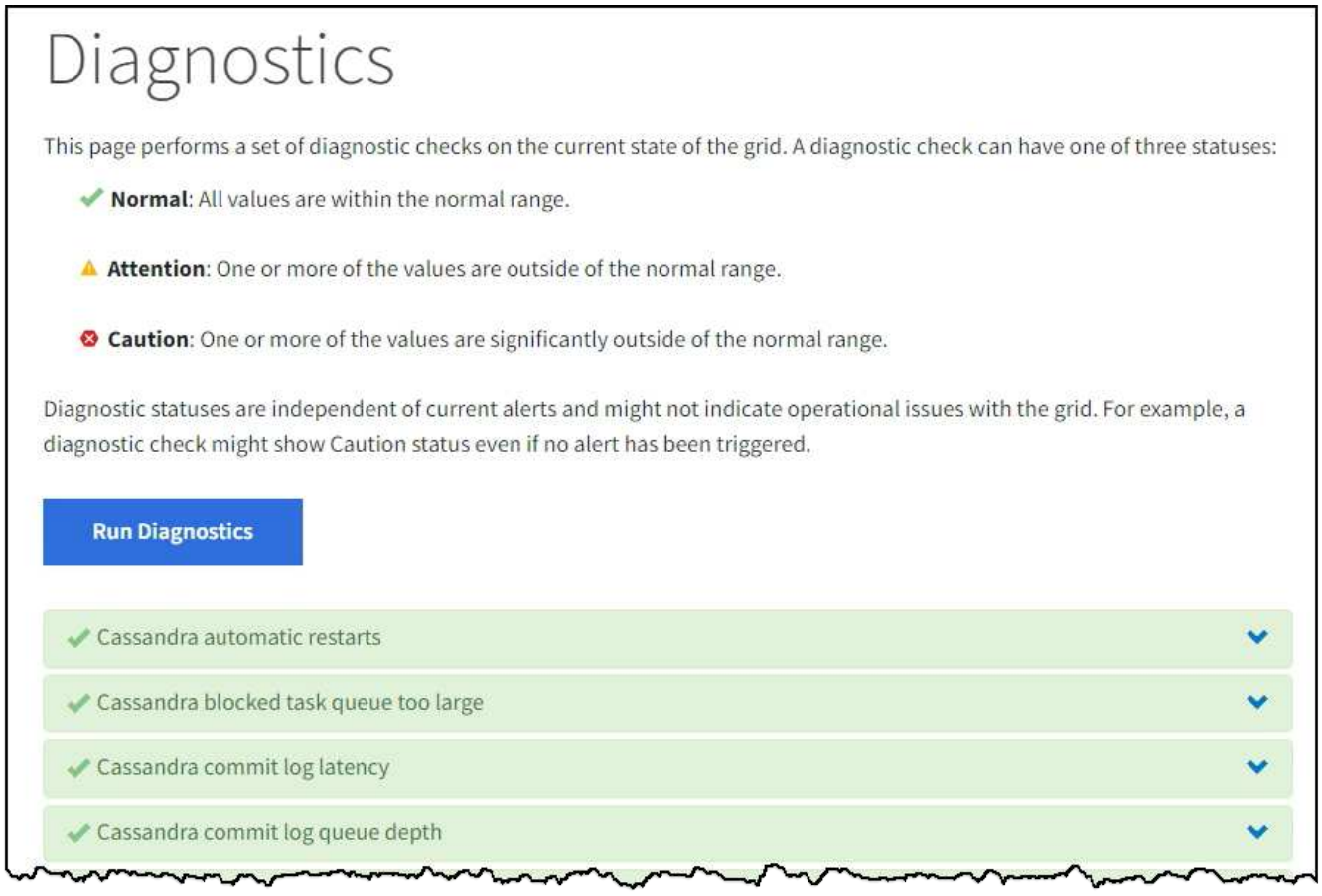
Os status de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a rede. Por exemplo, uma verificação de diagnóstico pode mostrar o status Cuidado mesmo que nenhum alerta tenha sido disparado.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Diagnóstico**.

   A página Diagnóstico é exibida e lista os resultados de cada verificação de diagnóstico. Os resultados são classificados por gravidade (Cuidado, Atenção e Normal). Dentro de cada gravidade, os resultados são classificados em ordem alfabética.

   Neste exemplo, todos os diagnósticos têm status Normal.



2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

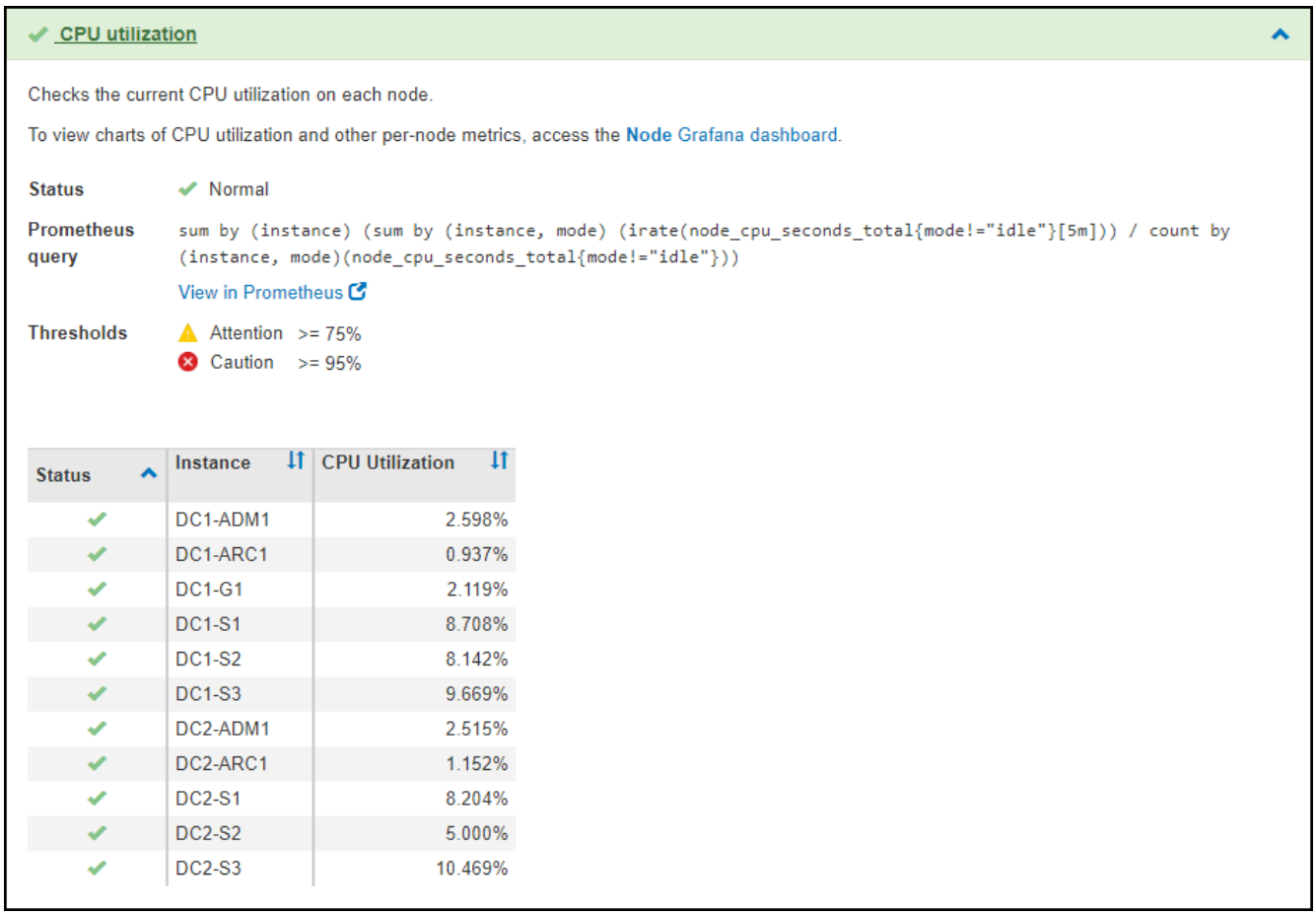
   Detalhes sobre o diagnóstico e seus resultados atuais aparecem. Os seguintes detalhes estão listados:

   - **Status**: O status atual deste diagnóstico: Normal, Atenção ou Cuidado.
   - **Consulta Prometheus**: Se usada para diagnóstico, a expressão Prometheus que foi usada para gerar os valores de status. (Uma expressão Prometheus não é usada para todos os diagnósticos.)

- **Limites**: Se disponíveis para o diagnóstico, os limites definidos pelo sistema para cada status de diagnóstico anormal. (Os valores limite não são usados para todos os diagnósticos.)

  > Você não pode alterar esses limites.

- **Valores de status**: Uma tabela que mostra o status e o valor do diagnóstico em todo o sistema StorageGRID . Neste exemplo, é mostrada a utilização atual da CPU para cada nó em um sistema StorageGRID . Todos os valores dos nós estão abaixo dos limites de Atenção e Cuidado, portanto, o status geral do diagnóstico é Normal.



3. **Opcional**: Para ver gráficos do Grafana relacionados a este diagnóstico, clique no link **Painel do Grafana**.

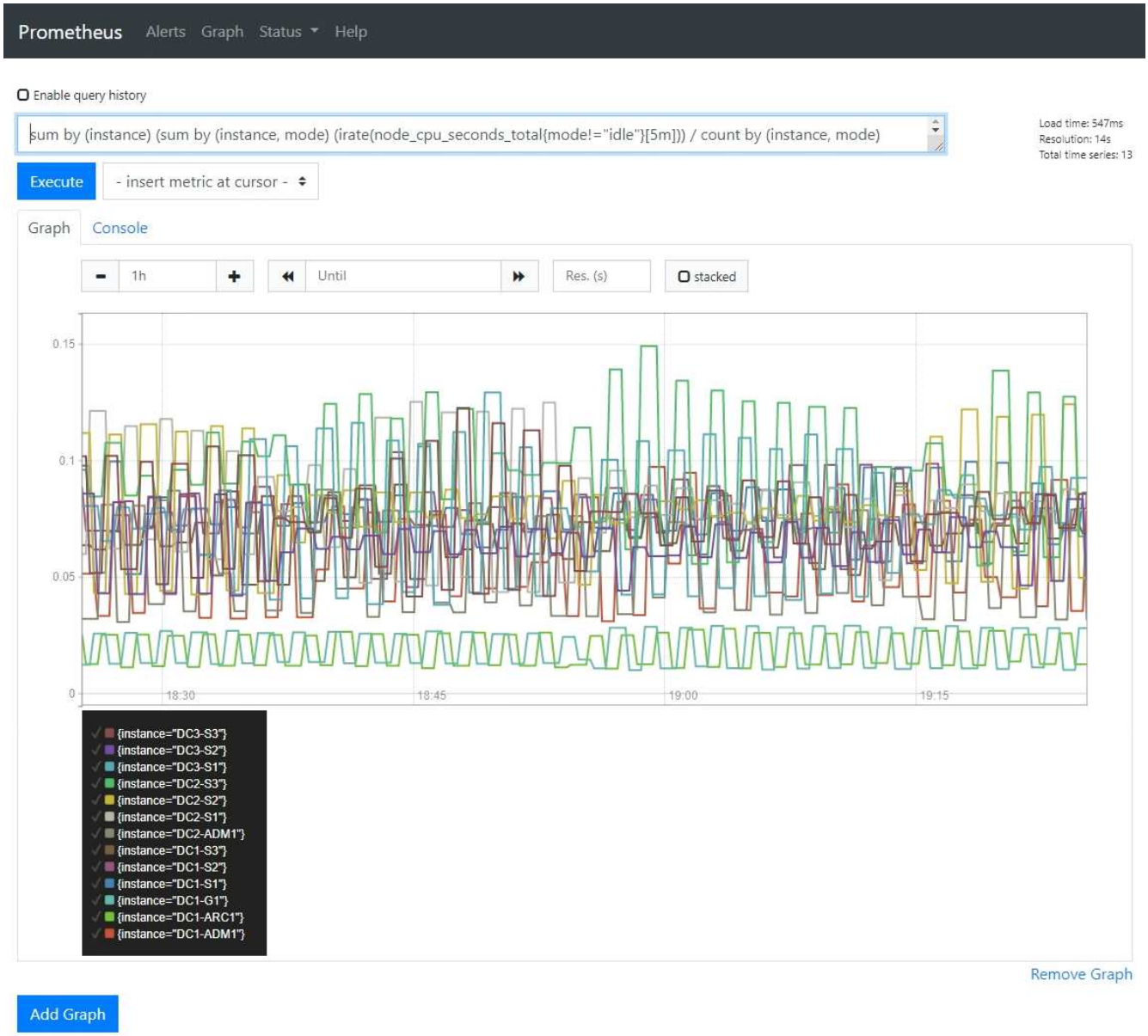
   Este link não é exibido para todos os diagnósticos.

   O painel relacionado do Grafana aparece. Neste exemplo, o painel do nó aparece mostrando a utilização da CPU ao longo do tempo para este nó, bem como outros gráficos do Grafana para o nó.

   > Você também pode acessar os painéis pré-construídos do Grafana na seção Grafana da página **SUPORTE** > **Ferramentas** > **Métricas**.

4. **Opcional**: Para ver um gráfico da expressão do Prometheus ao longo do tempo, clique em **Exibir no Prometheus**.

   Aparece um gráfico do Prometheus da expressão usada no diagnóstico.



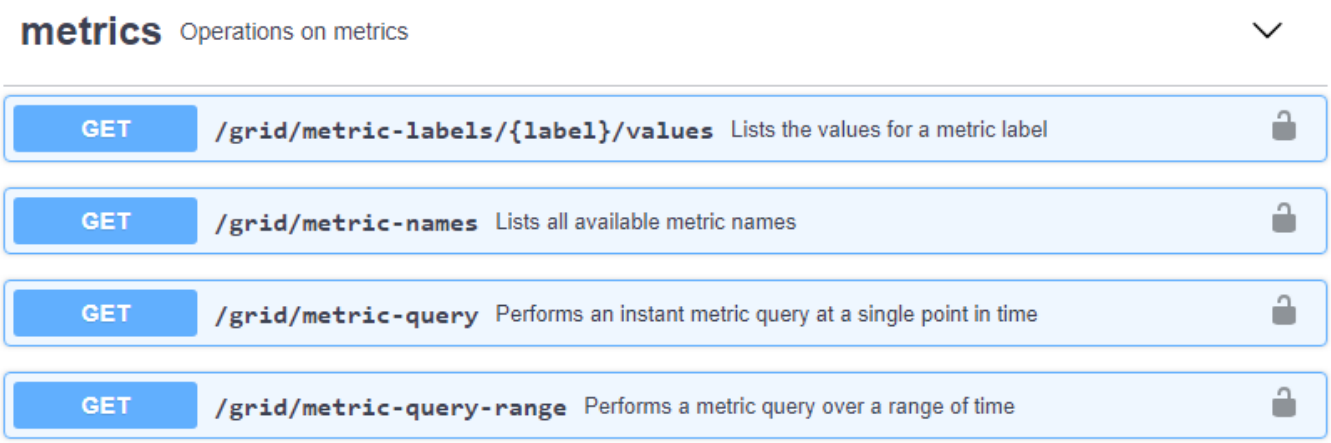
Crie aplicativos de monitoramento personalizados

Você pode criar aplicativos de monitoramento e painéis personalizados usando as métricas do StorageGRID disponíveis na API de gerenciamento de grade.

Se você quiser monitorar métricas que não são exibidas em uma página existente do Grid Manager ou se quiser criar painéis personalizados para o StorageGRID, poderá usar a API de gerenciamento de grade para consultar as métricas do StorageGRID .

Você também pode acessar as métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como o Grafana. O uso de uma ferramenta externa exige que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Veja o"instruções para administrar o StorageGRID" .

Para visualizar as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Grid Manager. No topo da página, selecione o ícone de ajuda e selecione **Documentação da API** > **métricas** .



Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo desta documentação.

Solucionar problemas do sistema StorageGRID

Solucionar problemas de um sistema StorageGRID

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

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

Defina o problema

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

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

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não fazendo? Quais são os sintomas?	Os aplicativos clientes estão relatando que objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez por volta das 14h50 do dia 8 de janeiro de 2020.
Como você percebeu o problema pela primeira vez?	Notificado pelo aplicativo do cliente. Também recebi notificações de alerta por e-mail.
O problema acontece constantemente ou apenas às vezes?	O problema continua.
Se o problema acontece regularmente, quais etapas fazem com que ele ocorra?	O problema acontece sempre que um cliente tenta ingerir um objeto.

Pergunta	Exemplo de resposta
Se o problema acontece intermitentemente, quando ele ocorre? Registre os horários de cada incidente que você tiver conhecimento.	O problema não é intermitente.
Você já viu esse problema antes? Com que frequência você teve esse problema no passado?	Esta é a primeira vez que vejo esse problema.

Avaliar o risco e o impacto no sistema

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

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

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

Coletar dados

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

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Criar cronograma de mudanças recentes	Alterações no seu sistema StorageGRID , sua configuração ou seu ambiente podem causar novos comportamentos.	• Crie uma linha do tempo das mudanças recentes

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Alertas de revisão	Os alertas podem ajudar você a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso. Revise a lista de alertas atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Revise os alertas acionados no passado para obter insights adicionais.	• "Ver alertas atuais e resolvidos"
Monitorar eventos	Eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas surgiram pela primeira vez e podem ajudar você a entender a rapidez com que as coisas estão mudando.	• "Use tabelas e gráficos" • "Usar relatórios de texto"
Estabelecer linhas de base	Colete informações sobre os níveis normais de vários valores operacionais. Esses valores de base e desvios dessas linhas de base podem fornecer pistas valiosas.	• Estabelecer linhas de base
Realizar testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com aqueles vistos ao usar o aplicativo cliente.	• "Monitore o desempenho de PUT e GET"
Revisar mensagens de auditoria	Revise as mensagens de auditoria para acompanhar as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Revisar mensagens de auditoria"
Verifique a localização dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de armazenamento.	• "Monitorar operações de verificação de objetos" • "Confirmar a localização dos dados do objeto" • "Verificar integridade do objeto"

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	• "Coletar arquivos de log e dados do sistema" • "Acionar manualmente um pacote AutoSupport" • "Revisar métricas de suporte"

Criar uma linha do tempo das mudanças recentes

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

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

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

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

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi instalado, expandido ou recuperado recentemente?
- O sistema foi atualizado recentemente? Foi aplicado algum hotfix?
- Algum hardware foi reparado ou trocado recentemente?
- A política do ILM foi atualizada?

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

Estabelecer linhas de base

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

Propriedade	Valor	Como obter
Consumo médio de armazenamento	GB consumidos/dia Porcentagem consumida/dia	Acesse o Gerenciador de Grade. Na página Nós, selecione a grade inteira ou um site e vá para a guia Armazenamento. No gráfico Armazenamento usado - Dados do objeto, encontre um período em que a linha seja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.

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

Propriedade	Valor	Como obter
Latência média de consulta	Milissegundos	Selecione **NÓS** > ***Nó de Armazenamento*** > **Objetos**. Na tabela Consultas, visualize o valor de Latência Média.

Analisar dados

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

A análise depende do problema, mas em geral:

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

Lista de verificação de informações de escalonamento

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

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, em que horários isso ocorreu? Defina o problema
	Avaliação de impacto	Qual é a gravidade do problema? Qual é o impacto no aplicativo cliente? • O cliente já se conectou com sucesso antes? • O cliente pode ingerir, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione **MANUTENÇÃO** > **Sistema** > **Licença**. O ID do sistema StorageGRID é exibido como parte da licença atual.
	Versão do software	Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Sobre** para ver a versão do StorageGRID .

✔	Item	Notas
	Personalização	Resuma como seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grade usa compactação de armazenamento, criptografia de armazenamento ou conformidade? • A ILM cria objetos replicados ou codificados para eliminação? O ILM garante redundância do site? As regras do ILM usam os comportamentos de ingestão Balanceado, Estrito ou Dual Commit?
	Arquivos de log e dados do sistema	Colete arquivos de log e dados do sistema para seu sistema. Selecione **SUPORTE** > **Ferramentas** > **Registros**. Você pode coletar logs para toda a grade ou para nós selecionados. Se você estiver coletando logs apenas para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de armazenamento em um site incluem o serviço ADC.) "Coletar arquivos de log e dados do sistema"
	Informações de base	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabelecer linhas de base
	Linha do tempo das mudanças recentes	Crie uma linha do tempo que resuma quaisquer alterações recentes no sistema ou em seu ambiente. Crie uma linha do tempo das mudanças recentes
	Histórico de esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, registre as etapas realizadas e o resultado.

Solucionar problemas de objetos e armazenamento

Confirmar a localização dos dados do objeto

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

Antes de começar

- Você deve ter um identificador de objeto, que pode ser um dos seguintes:

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

Passos

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

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

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

4. Selecione **Procurar**.

   O"resultados da pesquisa de metadados do objeto" aparecer. Esta página lista os seguintes tipos de informações:

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

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Falhas de armazenamento de objetos (volume de armazenamento)

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

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

Disk devices

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

Volumes

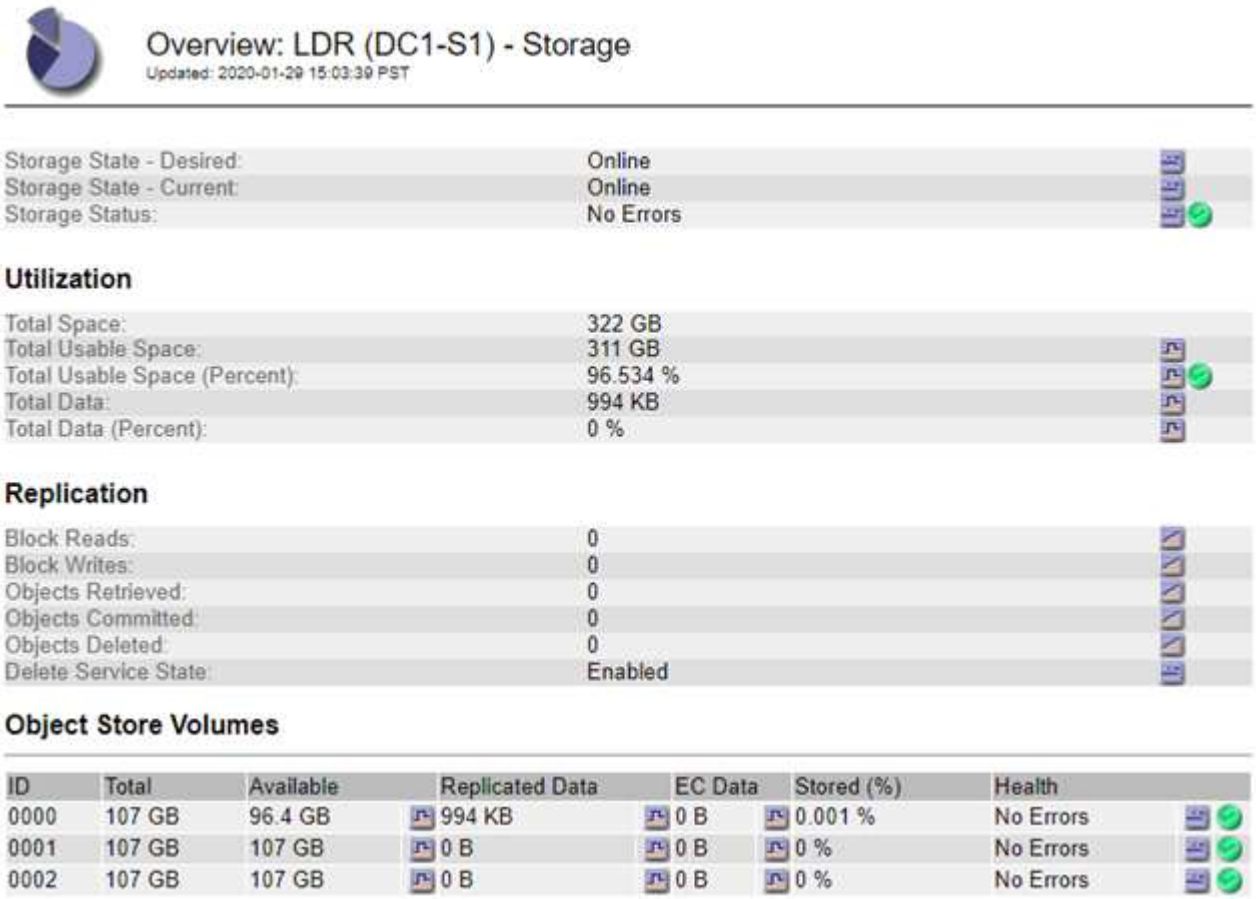
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

Object stores

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

Para ver mais"detalhes sobre cada nó de armazenamento" , siga estes passos:

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



Dependendo da natureza da falha, falhas em um volume de armazenamento podem ser refletidas em"alertas de volume de armazenamento" . Se um volume de armazenamento falhar, você deverá reparar o volume de armazenamento com falha para restaurar o Nó de Armazenamento à funcionalidade completa o mais rápido possível. Se necessário, você pode ir até a aba **Configuração** e"coloque o nó de armazenamento em um estado somente leitura" para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto você se prepara para uma recuperação completa do servidor.

Verificar integridade do objeto

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

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

O que é verificação de antecedentes?

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

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

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

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

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

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

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

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

Alertas relacionados à verificação de antecedentes

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

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

Alterar a taxa de verificação de antecedentes

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

Antes de começar

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

Sobre esta tarefa

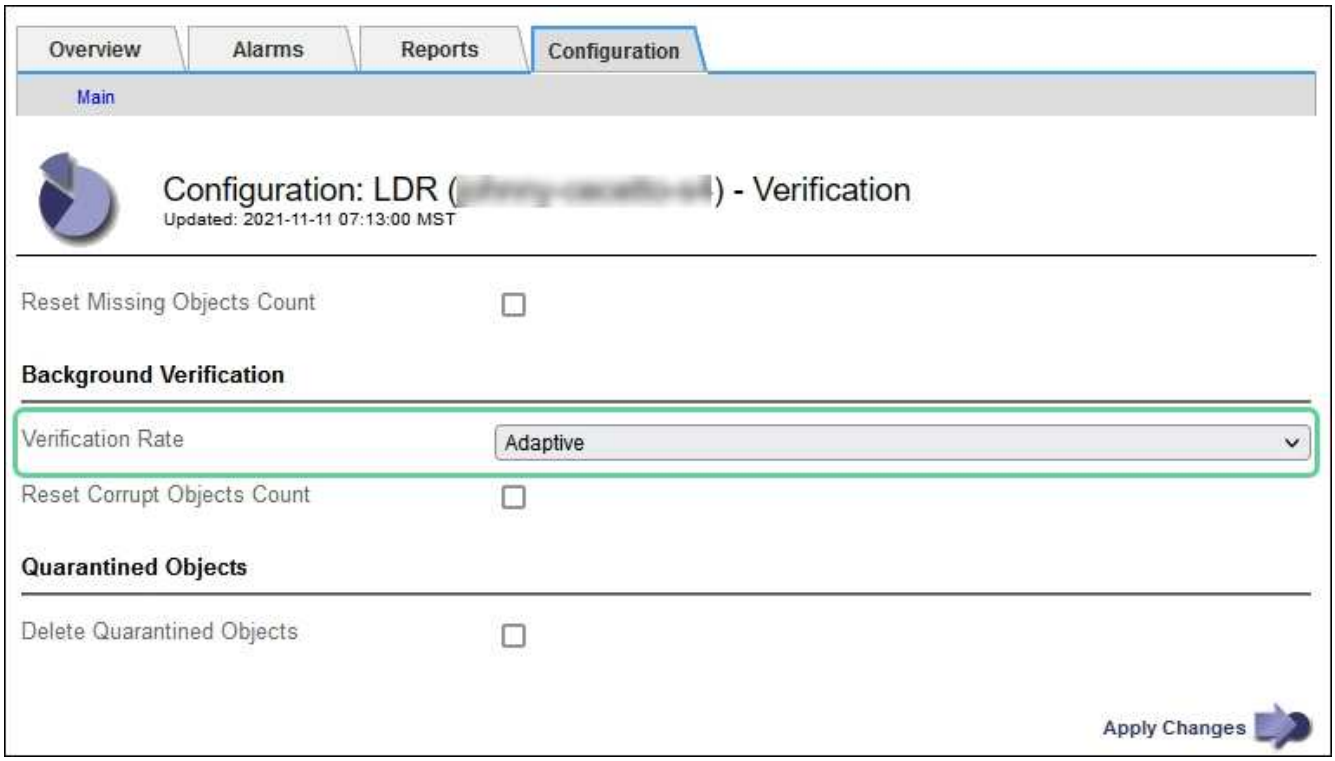
Você pode alterar a Taxa de Verificação para verificação em segundo plano em um Nó de Armazenamento:

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

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

Passos

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



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

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

      - Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova

cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar no sistema StorageGRID que satisfaça as políticas de ILM ativas.

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

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

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

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

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

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

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

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

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

O que é verificação de existência de objetos?

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

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

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

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

Executar verificação de existência de objeto

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

Antes de começar

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

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

Sobre esta tarefa

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

Passos

1. Selecione **MANUTENÇÃO** > **Tarefas** > **Verificação de existência de objeto**.
2. Selecione **Criar trabalho**. O assistente Criar uma tarefa de verificação de existência de objeto é exibido.
3. Selecione os nós que contêm os volumes que você deseja verificar. Para selecionar todos os nós on-line, marque a caixa de seleção **Nome do nó** no cabeçalho da coluna.

   Você pode pesquisar por nome do nó ou site.

Você não pode selecionar nós que não estejam conectados à grade.

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

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

6. Selecione **Continuar**.
7. Selecione a consistência para o trabalho.

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

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

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

8. Selecione **Continuar**.
9. Revise e verifique suas seleções. Você pode selecionar **Anterior** para ir para uma etapa anterior no assistente e atualizar suas seleções.

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

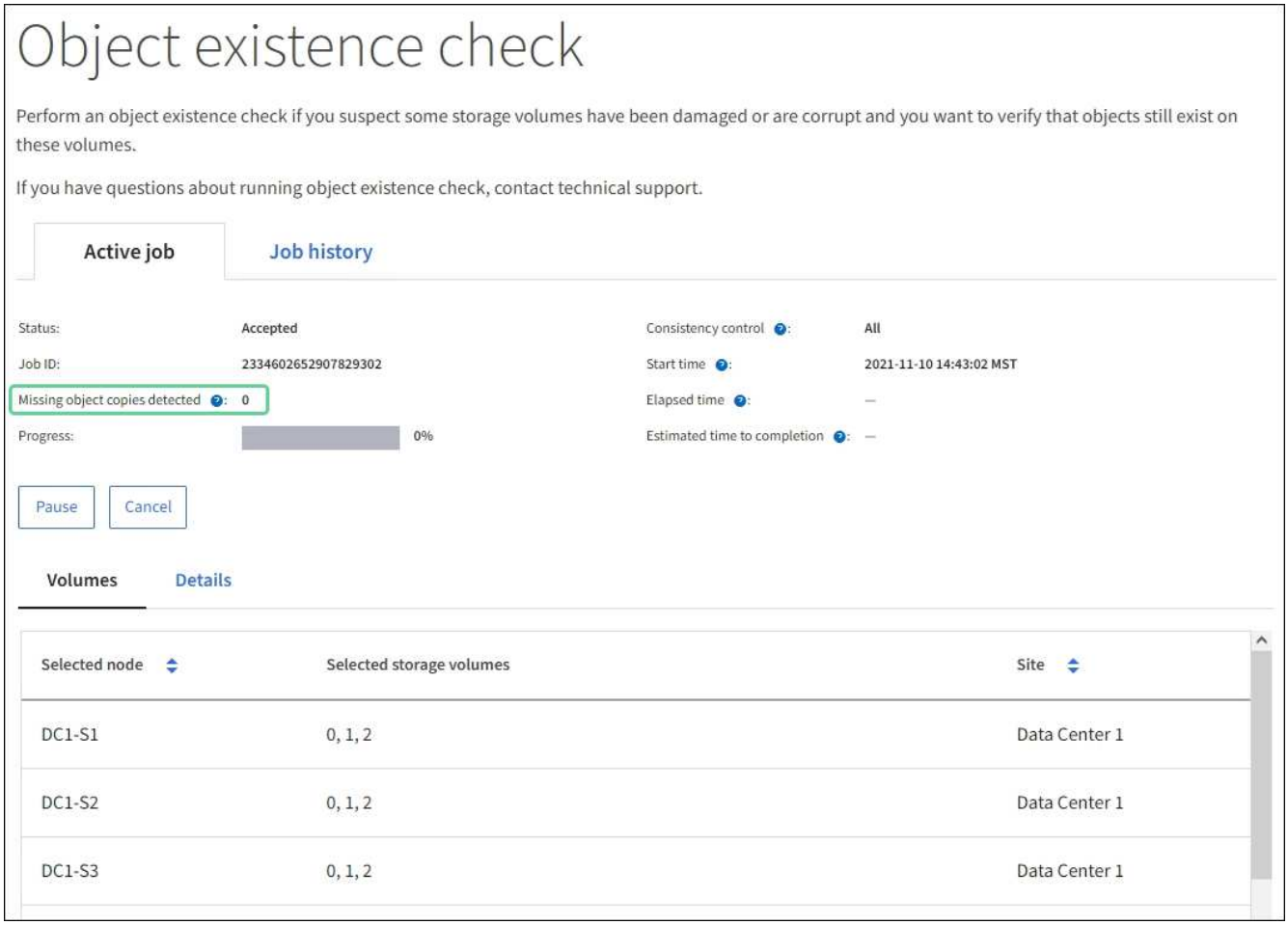
   - O trabalho foi concluído.
   - Você pausa ou cancela o trabalho. Você pode retomar um trabalho que foi pausado, mas não pode retomar um trabalho que foi cancelado.
   - O trabalho estagna. O alerta **A verificação de existência do objeto foi interrompida** é acionado. Siga as ações corretivas especificadas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

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

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

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

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



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

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

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

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

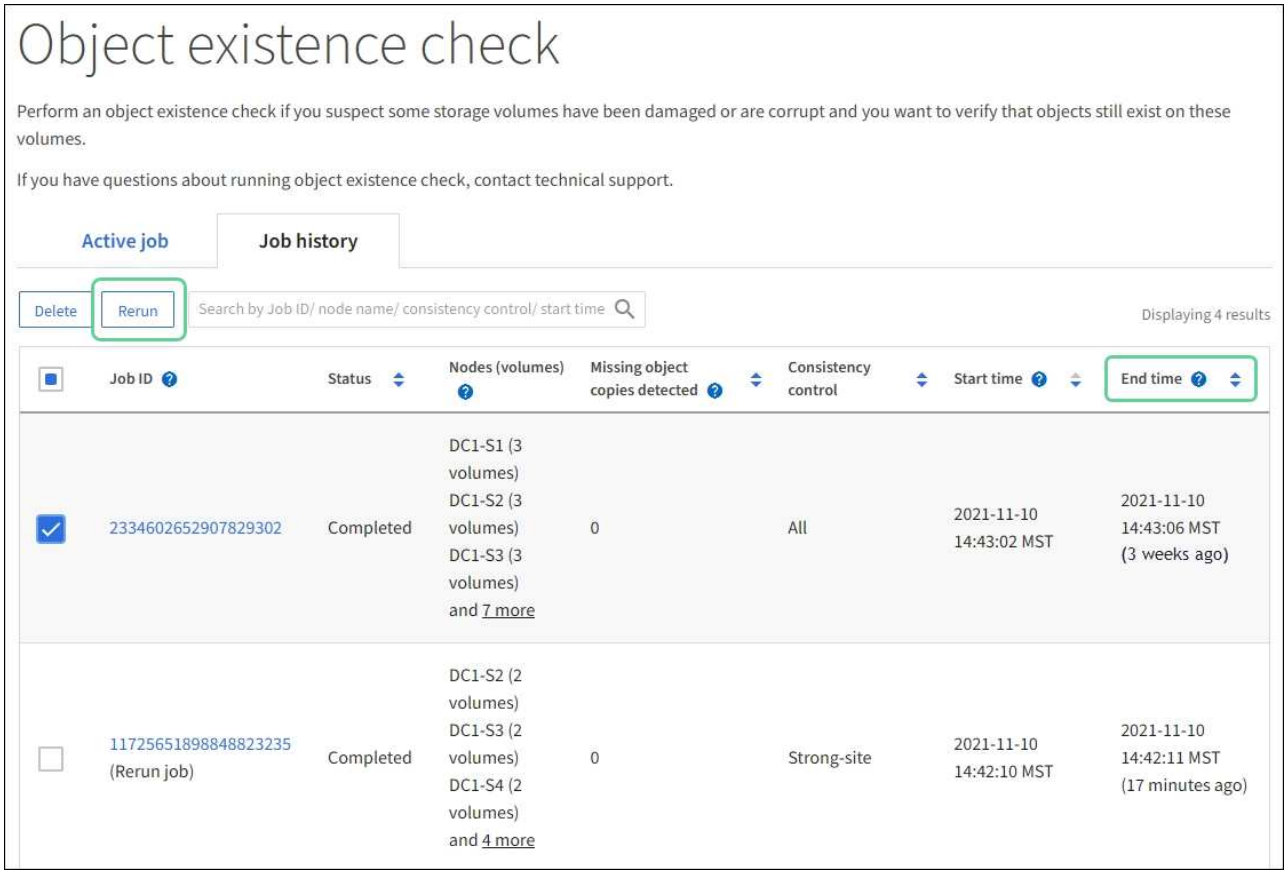
    a. Selecione **MANUTENÇÃO** > **Verificação de existência do objeto** > **Histórico de tarefas**.

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

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

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

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



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

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

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

Depois que você terminar

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

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

O alerta de tamanho de objeto S3 PUT muito grande é acionado se um locatário tentar uma operação PutObject não multiparte que exceda o limite de tamanho S3 de 5 GiB.

Antes de começar

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

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

Passos

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

   a. Digitar `ssh admin@primary_Admin_Node_IP`

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

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

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

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

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

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

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

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

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

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

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

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

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

Exemplo de resultados de log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][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):SPUT][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 identificá-lo:

   a. Vá para **SUPORTE** > **Ferramentas** > **Registros**. Colete logs de aplicativos para o nó de armazenamento no alerta. Especifique 15 minutos antes e depois do alerta.

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

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

   c. Pesquise no log por `method=PUT` e identificar o cliente no `clientIP` campo.

      Exemplo bycast.log

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

4. Informe aos locatários que o tamanho máximo do PutObject é 5 GiB e que devem usar uploads multipartes para objetos maiores que 5 GiB.

5. Ignore o alerta por uma semana se o aplicativo tiver sido alterado.

Solucionar problemas de dados de objetos perdidos e ausentes

Solucionar problemas de dados de objetos perdidos e ausentes

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

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

Se essa recuperação for bem-sucedida, o sistema StorageGRID substituirá a cópia ausente do objeto. Caso contrário, o alerta **Objetos perdidos** é acionado, da seguinte forma:

- Para cópias replicadas, se outra cópia não puder ser recuperada, o objeto será considerado perdido e o alerta será acionado.
- Para cópias codificadas para eliminação, se uma cópia não puder ser recuperada do local esperado, o atributo Cópias Corrompidas Detectadas (ECOR) será incrementado em um antes de uma tentativa de recuperar uma cópia de outro local. Se nenhuma outra cópia for encontrada, o alerta será disparado.

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

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

Investigar objetos perdidos

Quando o alerta **Objetos perdidos** for acionado, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em contato com o suporte técnico.

Antes de começar

- Você deve estar conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.

Sobre esta tarefa

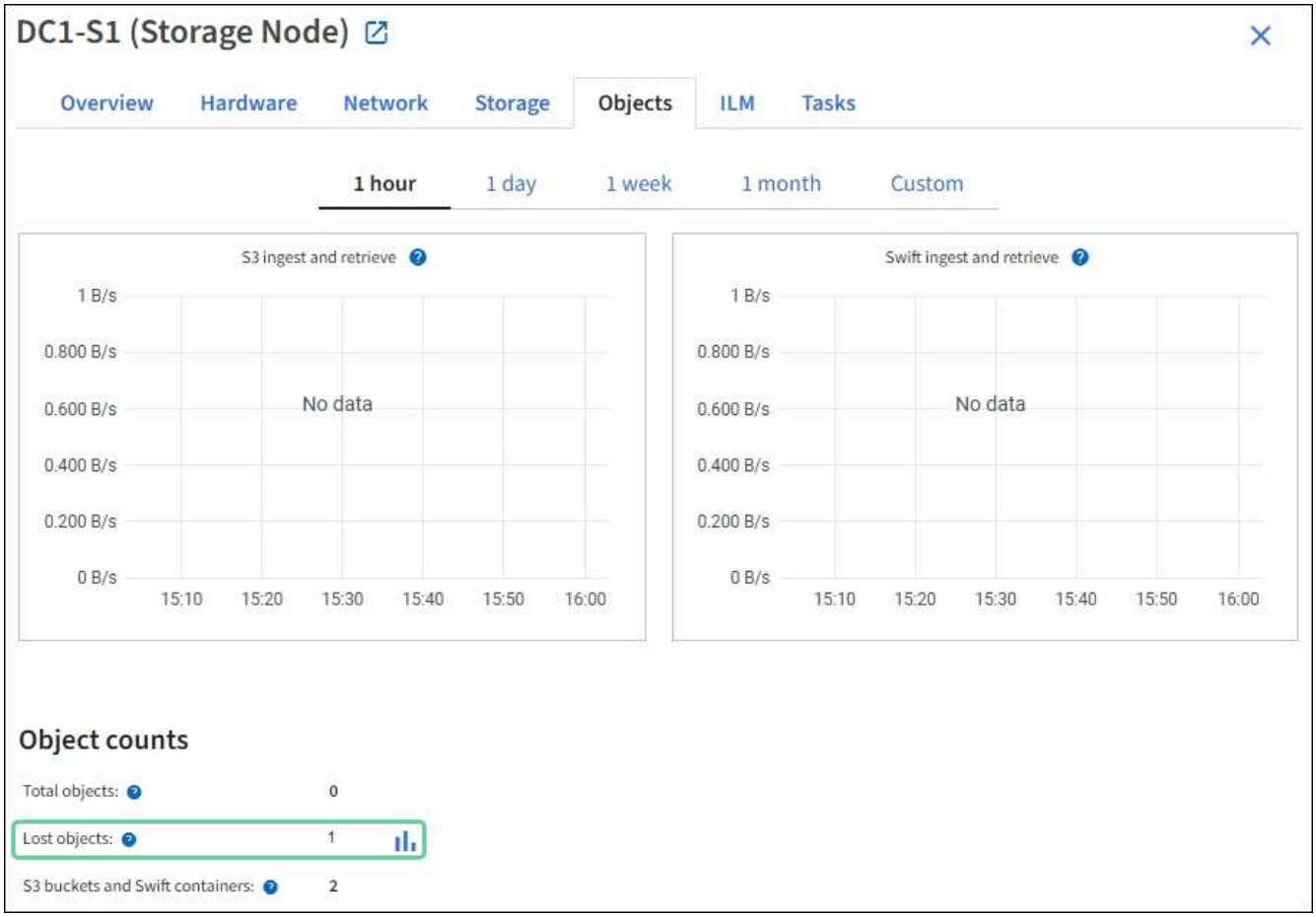
O alerta **Objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

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

Passos

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

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



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

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

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

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

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

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

d. Observe o valor do UUID incluído na mensagem.

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

5. Procure os metadados do objeto perdido usando o UUID:

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

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

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

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

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

Pesquisar e restaurar objetos potencialmente perdidos

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

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

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

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

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

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

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

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

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

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

Por exemplo:

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

d. Use grep para extrair as mensagens de auditoria de Localização Perdida (LLST) deste arquivo de saída. Digitar: `grep LLST output_file_name`

Por exemplo:

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

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

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

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

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

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

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

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

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

a. Efetue login no nó da grade:

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

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

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

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

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

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

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

Por exemplo, insira:

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

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

- Se o caminho do objeto não for encontrado, o objeto será perdido e não poderá ser restaurado usando este procedimento. Entre em contato com o suporte técnico.
- Se o caminho do objeto for encontrado, continue com a próxima etapa. Você pode tentar restaurar o objeto encontrado de volta para StorageGRID.

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

      Por exemplo, insira:

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

      Emitindo o `Object_Found` O comando notifica a grade sobre a localização do objeto. Ele também aciona as políticas ILM ativas, que fazem cópias adicionais conforme especificado em cada política.

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

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

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

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

        Continue com o próximo passo.

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

a. Efetue login no nó da grade:

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

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

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

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

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

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

   Por exemplo:

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

d. Use grep para extrair as mensagens de auditoria do Object Rules Met (ORLM) deste arquivo de saída. Digitar: `grep ORLM output_file_name`

   Por exemplo:

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

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

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

a. Encontre o campo LOCS na mensagem de auditoria.

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

6. "Redefinir a contagem de objetos perdidos e desaparecidos"no Gerenciador de Grade.

Redefinir contagens de objetos perdidos e desaparecidos

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos registrados foram perdidos permanentemente ou se é um alarme falso, você pode

redefinir o valor do atributo Objetos Perdidos para zero.

Antes de começar

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

Sobre esta tarefa

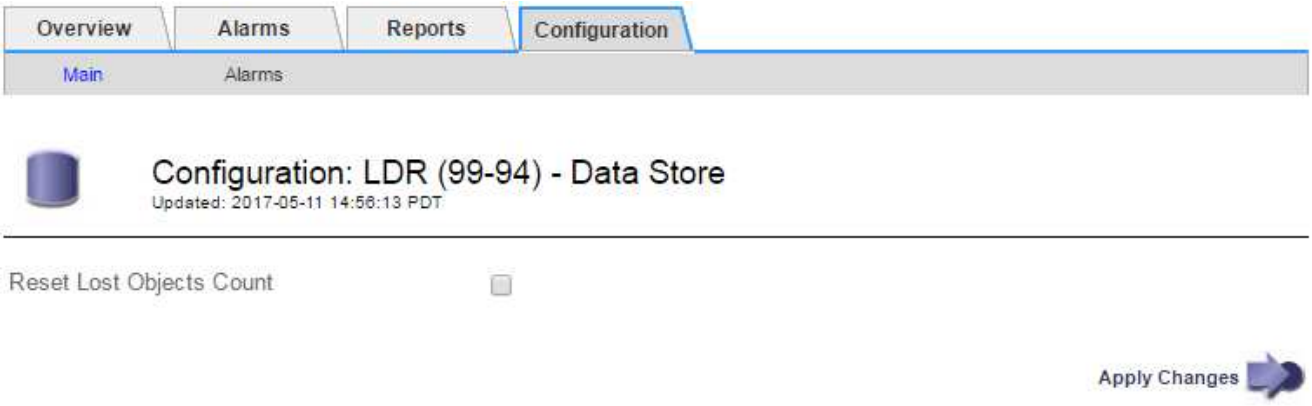
Você pode zerar o contador de Objetos Perdidos em qualquer uma das seguintes páginas:

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

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

Passos

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***Site*** > ***Nó de Armazenamento*** > **LDR** > **Armazenamento de Dados** > **Configuração** para o Nó de Armazenamento que tem o alerta **Objetos perdidos** ou o alarme PERDIDO.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **Aplicar alterações**.

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

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

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

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

   c. Clique em **Aplicar alterações**.

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

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

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

   Objetos em quarentena são criados quando a verificação em segundo plano identifica uma cópia corrompida do objeto replicado. Na maioria dos casos, o StorageGRID substitui automaticamente o objeto corrompido e é seguro excluir os objetos em quarentena. Entretanto, se o alerta **Objetos perdidos** ou o alarme PERDIDO for acionado, o suporte técnico pode querer acessar os objetos em quarentena.

g. Clique em **Aplicar alterações**.

Pode levar alguns instantes para que os atributos sejam redefinidos após você clicar em **Aplicar alterações**.

Solucionar problemas do alerta de armazenamento de dados de objeto baixo

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Nessa condição:

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

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

Passos

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

   A página Alertas é exibida.

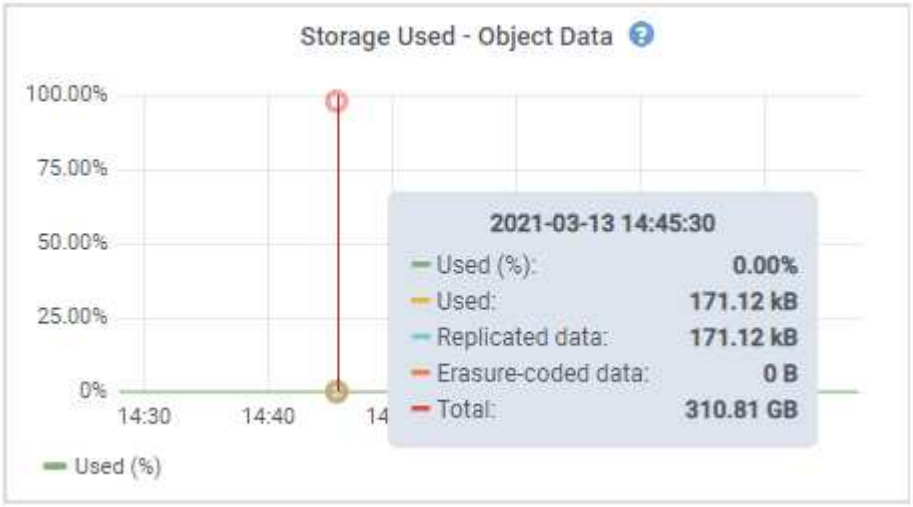
2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja visualizar.

Selecione o alerta, não o título de um grupo de alertas.

3. Revise os detalhes na caixa de diálogo e observe o seguinte:
   - Tempo acionado
   - O nome do site e do nó
   - Os valores atuais das métricas para este alerta
4. Selecione **NÓS** > ***Nó ou Site de Armazenamento*** > **Armazenamento**.
5. Posicione o cursor sobre o gráfico Armazenamento usado - Dados do objeto.

   Os seguintes valores são mostrados:

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



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

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

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

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

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

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

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

Em lançamentos anteriores, os três"marcas d'água de volume de armazenamento" eram configurações globais — os mesmos valores aplicados a cada volume de armazenamento em cada nó de armazenamento. A partir do StorageGRID 11.6, o software pode otimizar essas marcas d'água para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

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

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

Entenda o alerta

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

Cada instância do alerta indica que o valor personalizado da marca d'água somente leitura do volume de armazenamento é menor que o valor mínimo otimizado para esse nó de armazenamento. Se você continuar a usar a configuração personalizada, o Nó de Armazenamento poderá ficar com pouco espaço antes de poder fazer a transição segura para o estado somente leitura. Alguns volumes de armazenamento podem ficar inacessíveis (desmontados automaticamente) quando o nó atinge a capacidade.

Por exemplo, suponha que você tenha definido anteriormente a marca d'água somente leitura do volume de armazenamento para 5 GB. Agora suponha que o StorageGRID tenha calculado os seguintes valores otimizados para os quatro volumes de armazenamento no Nó de Armazenamento A:

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

O alerta **Substituição de marca d'água somente leitura baixa** é acionado para o Nó de Armazenamento A porque sua marca d'água personalizada (5 GB) é menor que o valor mínimo otimizado para todos os volumes

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

Resolva o alerta

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

Antes de começar

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

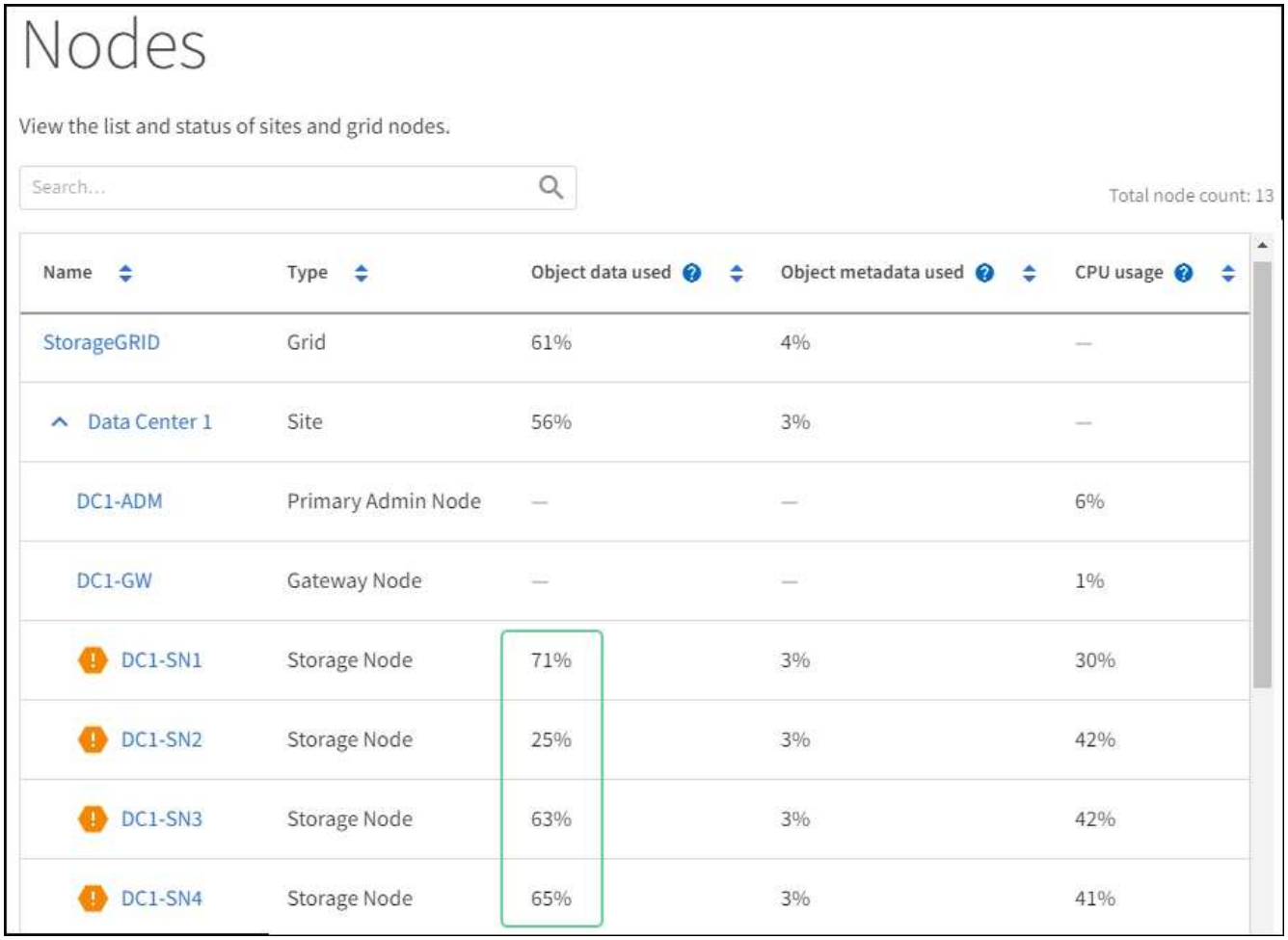
Sobre esta tarefa

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

Avalie o uso de dados do objeto para toda a grade

Passos

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



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

Ver marcas d'água de armazenamento otimizadas

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

Passos

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

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

Determine se você pode usar marcas d'água otimizadas

Passos

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

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

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

> ⓘ Os mesmos valores de marca d'água personalizados são aplicados a cada volume de armazenamento em cada nó de armazenamento. Usar valores menores que os recomendados para marcas d'água de volume de armazenamento pode fazer com que alguns volumes de armazenamento se tornem inacessíveis (desmontados automaticamente) quando o nó atingir a capacidade.

Use marcas d'água otimizadas

Passos

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

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

Solucionar problemas de metadados

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

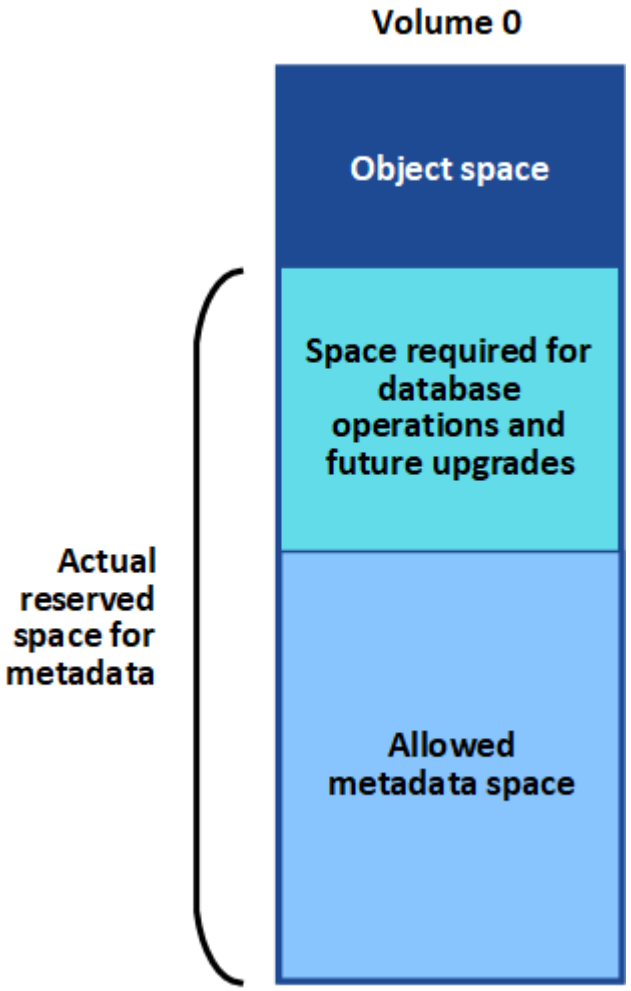
Antes de começar

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

Sobre esta tarefa

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

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



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

Você pode"monitorar a capacidade de metadados do objeto para cada nó de armazenamento" para ajudar você a antecipar erros e corrigi-los antes que eles ocorram.

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

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

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

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

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

Passos

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

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

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

Solucionar erros de certificado

Se você observar um problema de segurança ou de certificado ao tentar se conectar ao

StorageGRID usando um navegador da Web, um cliente S3 ou uma ferramenta de monitoramento externa, verifique o certificado.

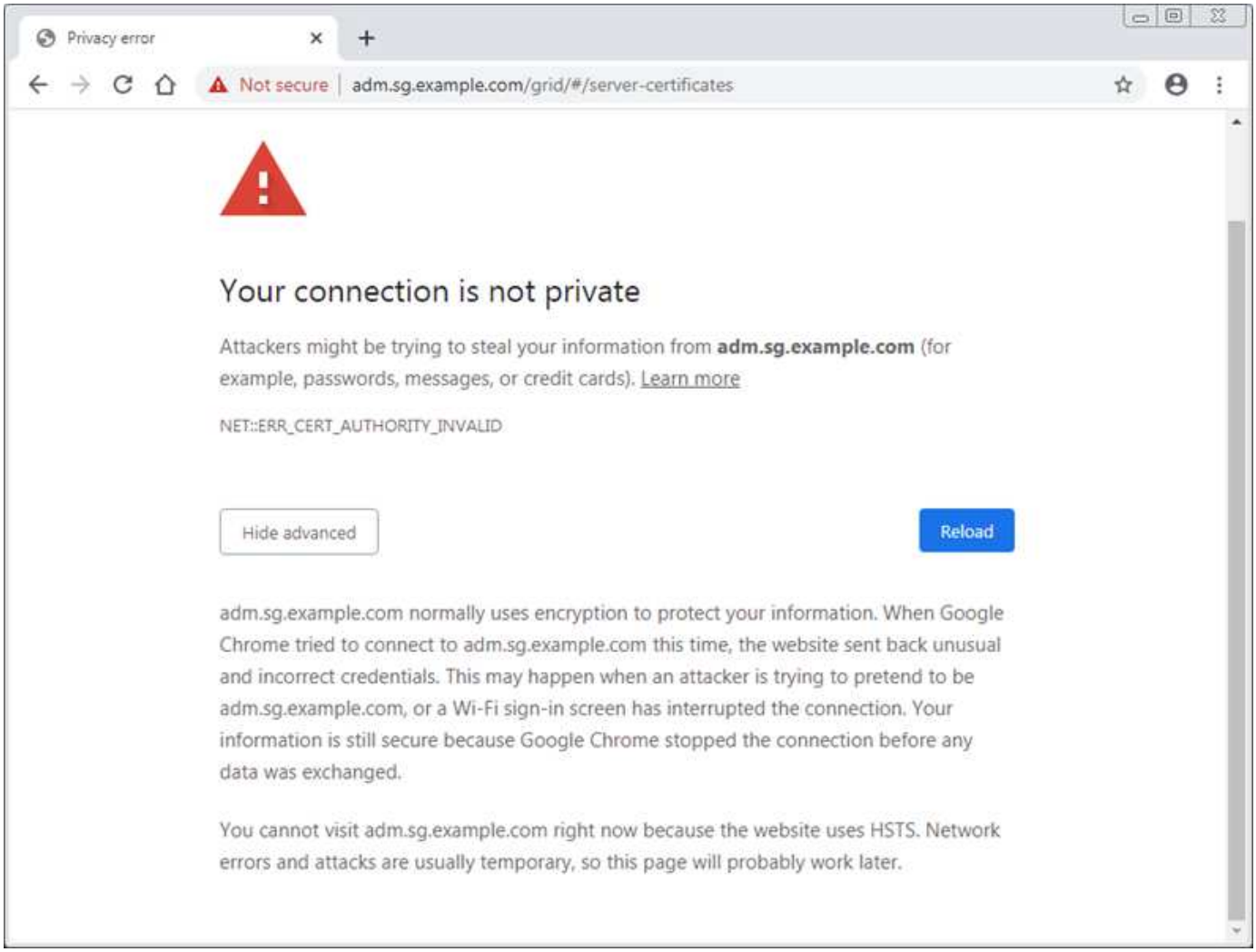
Sobre esta tarefa

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

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

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

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



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

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

Passos

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

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

Solucionar problemas do nó de administração e da interface do usuário

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

Erros de login do nó de administração

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

Antes de começar

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

Sobre esta tarefa

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

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

Passos

1. Aguarde 10 minutos e tente fazer login novamente.

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

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

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

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

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

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

   - Se o usuário local puder efetuar login:
     i. Revisar alertas.
     ii. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Federação de identidade**.
     iii. Clique em **Testar conexão** para validar suas configurações de conexão para o servidor LDAP.
     iv. Se o teste falhar, resolva quaisquer erros de configuração.
   - Se o usuário local não conseguir fazer login e você tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.
6. Use o Secure Shell (ssh) para efetuar login no nó de administração:
   a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

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

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

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

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

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

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

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

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

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

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

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

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

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

    Certifique-se de que os serviços idnt, acct, nginx e cassandra estejam todos em execução.
14. Repita os passosUse o Lenhador para coletar toras eRegistros de revisão para revisar os logs nos nós de armazenamento.
15. Se você não conseguir resolver o problema, entre em contato com o suporte técnico.

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

Problemas de interface do usuário

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

Passos

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

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

Solucionar problemas de rede, hardware e plataforma

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

Erros "422: Entidade não processável"

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

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

Mensagem de erro	Causa raiz e ação corretiva

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

Mensagem de erro	Causa raiz e ação corretiva

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

Alerta de incompatibilidade de MTU da rede de grade

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

Sobre esta tarefa

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

Passos

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

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

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

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

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

+

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

Alerta de erro de quadro de recepção de rede de nó

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

Sobre esta tarefa

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

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

Passos

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

Incompatibilidade de FEC

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

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

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

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

Incompatibilidade de porta do switch e MTU da placa de rede

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

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

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

Veja também "Alterar configuração de MTU" .

Altas taxas de erro de link

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

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

Estouro do buffer de anel da placa de rede

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

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

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

Erros de sincronização de tempo

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

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

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

Linux: Problemas de conectividade de rede

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

Clonagem de endereço MAC

Em alguns casos, problemas de rede podem ser resolvidos usando clonagem de endereço MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereço MAC para cada uma das suas redes como "true" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do

contêiner StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções para"Red Hat Enterprise Linux" ou"Ubuntu ou Debian" .

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

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

Modo promíscuo

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

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

Linux: o status do nó é "órfão"

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

Sobre esta tarefa

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

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

Passos

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

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

   Se o nó for órfão, a resposta é

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

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

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

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

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

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

Linux: Solucionar problemas de suporte a IPv6

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

Sobre esta tarefa

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

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

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

Passos

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

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

   O resultado deve ser 0.

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

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

3. Digite o contêiner do nó StorageGRID : `storagegrid node enter node-name`
4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

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

O resultado deve ser 1.

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

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

5. Sair do contêiner: `exit`

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

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

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

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

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

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

8. Execute estes comandos para reiniciar o contêiner StorageGRID :

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

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

Solucionar problemas de um servidor syslog externo

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

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

Problemas em tempo de execução podem ser relatados pelo"Erro de encaminhamento do servidor syslog

externo" alerta. Se você receber este alerta, siga as instruções no alerta para reenviar as mensagens de teste para que você possa obter mensagens de erro detalhadas.

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

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

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

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

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

Revisar logs de auditoria

Mensagens e logs de auditoria

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e dos logs de auditoria do StorageGRID . Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções são para administradores responsáveis por produzir relatórios de atividade e uso do sistema

que exigem análise das mensagens de auditoria do sistema StorageGRID .

Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó de administração.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, consulte"Configurar mensagens de auditoria e destinos de log" .

Fluxo e retenção de mensagens de auditoria

Todos os serviços do StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para o `audit.log` arquivo.

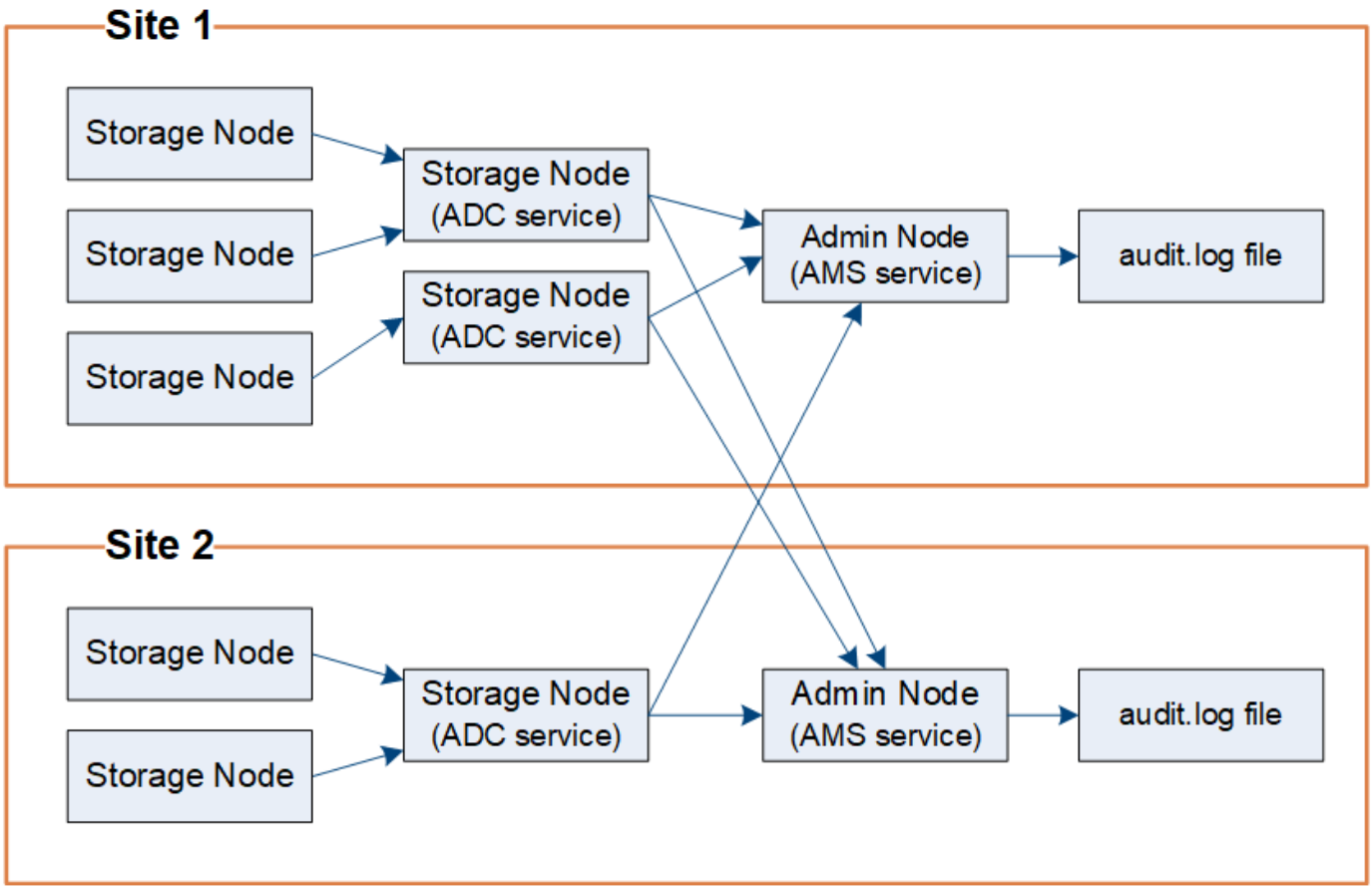
Fluxo de mensagens de auditoria

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços do ADC no site do data center. O serviço ADC é habilitado automaticamente para os três primeiros nós de armazenamento instalados em cada site.

Por sua vez, cada serviço ADC atua como um retransmissor e envia sua coleção de mensagens de auditoria para cada nó administrativo no sistema StorageGRID , o que fornece a cada nó administrativo um registro completo da atividade do sistema.

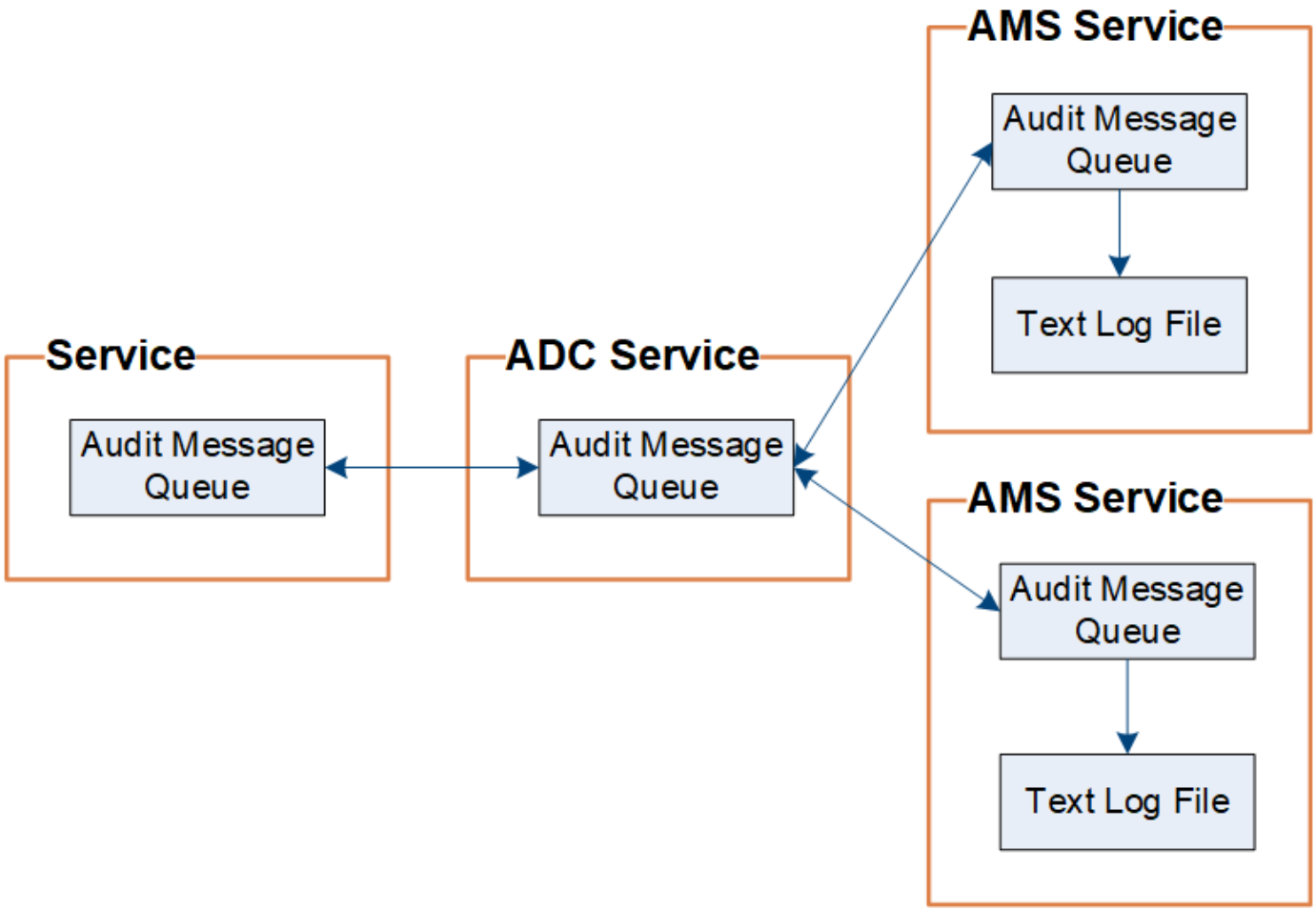
Cada nó de administração armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é denominado `audit.log` .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de copiar e excluir para garantir que nenhuma mensagem de auditoria seja perdida antes de ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no nó de administração. `/var/local/log` diretório. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conectividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível em cada nó `/var/local/` diretório. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/log` o diretório usado por um nó de administração ficar cheio, o nó de administração será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações do cliente S3 não são afetadas. O alarme XAMS (Repositórios de auditoria inacessíveis) é acionado quando um repositório de auditoria fica inacessível.
- Se o `/var/local/` o diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para mensagens de auditoria até que o diretório esteja apenas 87% cheio. As solicitações do cliente S3 para outros nós não são afetadas. O alarme NRLY (Relés de auditoria disponíveis) é acionado quando os relés de auditoria estão inacessíveis.

> Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente no `/var/local/log/localaudit.log` arquivo.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria fiquem muito grandes:

- A interrupção de um nó de administração ou de um nó de armazenamento com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes poderão ficar acumulados.
- Uma taxa de atividade sustentada que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC ficando cheio por motivos não relacionados a mensagens de auditoria. Quando isso acontece, o nó para de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria na fila (AMQS)

Para ajudar você a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **Fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administração atinge determinados limites.

Se o alerta **Grande fila de auditoria** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema. Se houver um número significativo de transações recentes, o alerta e o alarme deverão ser resolvidos com o tempo e poderão ser ignorados.

Se o alerta ou alarme persistir e aumentar em gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para Gravações do Cliente e Leituras do Cliente para Erro ou Desligado. Ver "Configurar mensagens de auditoria e destinos de log" .

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora caso ocorra uma falha de rede ou nó. Por esse motivo, podem existir mensagens duplicadas no log de auditoria.

Arquivo de log de auditoria de acesso

O compartilhamento de auditoria contém o ativo `audit.log` arquivo e quaisquer arquivos de log de auditoria compactados. Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó de administração.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP de um nó de administração.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

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

2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/log
```

3. Visualize o arquivo de log de auditoria atual ou salvo, conforme necessário.

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos em um nó de administração `/var/local/log` diretório. Os arquivos de log de auditoria ativos são nomeados `audit.log` .

> Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver "Configurar mensagens de auditoria e destinos de log" .

Uma vez por dia, o ativo `audit.log` o arquivo é salvo e um novo `audit.log` o arquivo é iniciado. O nome do arquivo salvo indica quando ele foi salvo, no formato *`yyyy-mm-dd.txt`* . Se mais de um log de auditoria for criado em um único dia, os nomes dos arquivos usarão a data em que o arquivo foi salvo, anexada por um número, no formato *`yyyy-mm-dd.txt.n`* . Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são o primeiro e o segundo arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`* , que preserva a data original. Com o tempo, isso resulta no consumo de armazenamento alocado para logs de auditoria no nó de administração. Um script monitora o consumo de espaço do log de auditoria e exclui os arquivos de log conforme necessário para liberar espaço no `/var/local/log` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log` .

Este exemplo mostra o ativo `audit.log` arquivo, arquivo do dia anterior(`2018-04-15.txt`), e o arquivo compactado do dia anterior(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato de arquivo de log de auditoria

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó administrativo e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O Tempo Universal Coordenado (UTC) do evento que disparou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido por um espaço:

YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* são microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT` .

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para facilitar a leitura). Essas mensagens foram geradas quando um locatário criou um bucket S3 e adicionou dois objetos a esse bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

No formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou

interpretar. Você pode usar o"ferramenta audit-explain" para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar o"ferramenta de soma de auditoria" para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

Use a ferramenta audit-explain

Você pode usar o `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria para um formato fácil de ler.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-explain` A ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.

> O `audit-explain` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-explain` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-explain` ferramenta. Esses quatro"CUSPIR" mensagens de auditoria foram geradas quando o locatário do S3 com ID de conta 92484777680322627870 usou solicitações S3 PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

O `audit-explain` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Processe vários arquivos simultaneamente. Por exemplo:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep SPUT audit.log | audit-explain

grep bucket-name audit.log | audit-explain
```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando as partes que deseja examinar e executando `audit-explain` nas partes, em vez do arquivo inteiro.

> O `audit-explain` a ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .
2. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   O `audit-explain` A ferramenta imprime interpretações legíveis por humanos de todas as mensagens no arquivo ou arquivos especificados.

   > Para reduzir o comprimento das linhas e facilitar a leitura, os registros de data e hora não são exibidos por padrão. Se você quiser ver os carimbos de data/hora, use o carimbo de data/hora(`-t`) opção.

Use a ferramenta audit-sum

Você pode usar o `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e para ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-sum` A ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

> O `audit-sum` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-sum` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

O `audit-sum` A ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria do S3, Swift e ILM em um log de auditoria.

> Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Documentação da ferramenta de soma de auditoria do StorageGRID 11.8" .

Código	Descrição	Consulte
IDEL	Exclusão iniciada pelo ILM: registra quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket.	"SDEL: S3 EXCLUIR"

Código	Descrição	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 OBTER"
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: CABEÇA S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	"WDEL: Swift EXCLUIR"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	"WHEA: CABEÇA Rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	"WPUT: PUT rápido"

O `audit-sum` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Processe vários arquivos simultaneamente. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

Esta ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Você pode usar opções de linha de comando para resumir operações em buckets separadamente de operações em objetos ou para agrupar resumos de mensagens por nome de bucket, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo mínimo, máximo e médio de operação, mas você pode usar o `size (-s)` opção para olhar o tamanho do objeto.

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

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

2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
   a. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Neste exemplo, as operações SGET (S3 GET) são as mais lentas, em média, com 1,13 segundos, mas as operações SGET e SPUT (S3 PUT) mostram tempos longos de pior caso, de cerca de 1.770 segundos.

b. Para mostrar as 10 operações de recuperação mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicione a opção de saída longa(`-l`) para incluir caminhos de objetos:

   ```
   grep SGET audit.log | audit-sum -l
   ```

   Os resultados incluem o tipo (objeto ou bucket) e o caminho, o que permite que você pesquise no log de auditoria outras mensagens relacionadas a esses objetos específicos.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
A partir deste exemplo de saída, você pode ver que as três solicitações GET do S3 mais lentas foram para objetos com cerca de 5 GB de tamanho, o que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos no pior caso.

3. Se você quiser determinar quais tamanhos de objetos estão sendo ingeridos e recuperados de sua grade, use a opção de tamanho(`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior que o número de mensagens SGET, indicando que a maioria dos objetos nunca é recuperada.

4. Se você quiser determinar se as recuperações foram lentas ontem:

   a. Emita o comando no log de auditoria apropriado e use a opção group-by-time(`-gt`), seguido pelo período de tempo (por exemplo, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Esses resultados mostram que o tráfego S3 GET atingiu o pico entre 06:00 e 07:00. Os tempos máximo e médio também são consideravelmente maiores nesses momentos e não aumentam gradualmente conforme a contagem aumenta. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

b. Para determinar o tamanho dos objetos que foram recuperados a cada hora ontem, adicione a opção de tamanho(`-s`) ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no máximo.

c. Para ver mais detalhes, use o"ferramenta audit-explain" para revisar todas as operações do SGET durante aquela hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando grep for esperada em muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) por vez.

5. Se você quiser determinar se as operações SPUT em buckets são mais lentas do que as operações SPUT para objetos:

a. Comece usando o `-go` opção, que agrupa mensagens para operações de objeto e bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Os resultados mostram que as operações SPUT para buckets têm características de desempenho diferentes das operações SPUT para objetos.

b. Para determinar quais buckets têm as operações SPUT mais lentas, use o `-gb` opção, que agrupa mensagens por bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                 count     min(sec)        max(sec)
average(sec)
  =============                 =====     ========        ========
============
  SPUT.cho-non-versioning       71943        0.046        1770.563
1.571
  SPUT.cho-versioning           54277        0.047        1736.633
1.415
  SPUT.cho-west-region          80615        0.040          55.557
1.329
  SPUT.ldt002                 1564563        0.011          51.569
0.361
```

c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use ambos `-gb` e o `-s` opções:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato de mensagem de auditoria

Formato de mensagem de auditoria

As mensagens de auditoria trocadas dentro do sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico descrevendo o evento ou atividade que está sendo relatada.

Se as informações resumidas fornecidas pelo"auditoria-explicação" e"soma de auditoria" ferramentas for insuficiente, consulte esta seção para entender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Cada mensagem de auditoria contém uma sequência de elementos de atributo. A sequência inteira está entre colchetes(`[ ]`), e cada elemento de atributo na string tem as seguintes características:

- Entre parênteses `[ ]`
- Introduzido pela corda `AUDT` , que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de quebra de linha `\n`

Cada elemento inclui um código de atributo, um tipo de dado e um valor que são relatados neste formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

O número de elementos de atributo na mensagem depende do tipo de evento da mensagem. Os elementos de atributo não são listados em nenhuma ordem específica.

A lista a seguir descreve os elementos de atributo:

- `ATTR`é um código de quatro caracteres para o atributo que está sendo relatado. Há alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos do evento.
- `type`é um identificador de quatro caracteres do tipo de dados de programação do valor, como UI64, FC32 e assim por diante. O tipo está entre parênteses `( ) .
- `value`é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores sempre seguem dois pontos (:`). Valores do tipo de dados CSTR são colocados entre aspas duplas " ".

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo sem sinal (32 bits); pode armazenar os números de 0 a 4.294.967.295.
UI64	Inteiro duplo longo sem sinal (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro caracteres; um valor inteiro sem sinal de 32 bits representado como quatro caracteres ASCII, como "ABCD".
iPad	Usado para endereços IP.
CSTR	Uma matriz de comprimento variável de caracteres UTF-8. Os caracteres podem ser escapados com as seguintes convenções: • A barra invertida é \\. • O retorno de carro é \r. • Aspas duplas são \". • A quebra de linha (nova linha) é \n. • Os caracteres podem ser substituídos por seus equivalentes hexadecimais (no formato \xHH, onde HH é o valor hexadecimal que representa o caractere).

Dados específicos do evento

Cada mensagem de auditoria no log de auditoria registra dados específicos de um evento do sistema.

Após a abertura `[AUDT:` contêiner que identifica a mensagem em si, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrita pela mensagem de auditoria. Esses atributos são destacados no

exemplo a seguir:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"conta"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJ
A=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"conta"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"objeto"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o"KARITÉ" código de mensagem ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação S3 HEAD bem-sucedida.

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
ENTRE	FC32	ID do módulo: um identificador de quatro caracteres do ID do módulo que gerou a mensagem. Isso indica o segmento de código no qual a mensagem de auditoria foi gerada.
ANID	UI32	ID do nó: ID do nó da grade atribuído ao serviço que gerou a mensagem. Cada serviço recebe um identificador exclusivo no momento em que o sistema StorageGRID é configurado e instalado. Este ID não pode ser alterado.
ASES	UI64	Identificador de Sessão de Auditoria: Em versões anteriores, esse elemento indicava o horário em que o sistema de auditoria foi inicializado após o serviço ser iniciado. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). **Observação:** Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: em versões anteriores, esse contador era incrementado para cada mensagem de auditoria gerada no nó da grade (ANID) e zerado na reinicialização do serviço. **Observação:** Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: um identificador compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.

Código	Tipo	Descrição
ATIM	UI64	Carimbo de data/hora: hora em que o evento foi gerado e que disparou a mensagem de auditoria, medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o registro de data e hora em data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o registro de data e hora registrado. O tempo legível por humanos que aparece no início da mensagem de auditoria no `audit.log` arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , onde o `T` é um caractere de sequência literal que indica o início do segmento de tempo da data. *`UUUUUU`* são microssegundos.
ATYP	FC32	Tipo de evento: um identificador de quatro caracteres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: os atributos que são incluídos.
MÉDIO	UI32	Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade com versões anteriores no serviço AMS para processar mensagens de versões mais antigas dos serviços.
RSLT	FC32	Resultado: O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é usado em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no `audit.log` arquivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo registrado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é registrado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

O valor do atributo ATYP é SPUT. "CUSPIR" representa uma transação S3 PUT, que registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o bucket ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Para descobrir quando o evento PUT ocorreu, observe o registro de data e hora do Tempo Universal Coordenado (UTC) no início da mensagem de auditoria. Este valor é uma versão legível do atributo ATIM da própria mensagem de auditoria:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

O ATIM registra o tempo, em microssegundos, desde o início da era UNIX. No exemplo, o valor `1405631878959669` traduz para quinta-feira, 17-jul-2014 21:17:59 UTC.

Mensagens de auditoria e o ciclo de vida do objeto

Quando as mensagens de auditoria são geradas?

Mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API do S3.

As mensagens de auditoria são vinculadas por meio de identificadores específicos para cada protocolo.

Protocolo	Código
Vinculando operações S3	S3BK (balde), S3KY (chave) ou ambos
Vinculando operações Swift	WCON (contêiner), WOBJ (objeto) ou ambos
Vinculando operações internas	CBDID (identificador interno do objeto)

Cronometragem das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós da grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar daquela mostrada nos exemplos desta seção.

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão estão listadas nas tabelas a seguir. Somente as mensagens necessárias para rastrear a transação de ingestão são incluídas.

Mensagens de auditoria de ingestão do S3

Código	Nome	Descrição	Rastro	Ver
CUSPIR	Transação S3 PUT	Uma transação de ingestão S3 PUT foi concluída com sucesso.	CBDI, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Rastro	Ver
WPUT	Transação Swift PUT	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBDI, WCON, WOBJ	"WPUT: PUT rápido"

Código	Nome	Descrição	Rastro	Ver
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Exemplo: ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente S3 ingere um objeto em um nó de armazenamento (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM Fazer 2 Cópias.

> Nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de ingestão S3 (SPUT) são listados.

Este exemplo pressupõe que um bucket S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um bucket específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regras de Objeto Atendidas

A mensagem ORLM indica que a política ILM foi satisfeita para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM que foi aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume dos locais do objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Para objetos codificados por eliminação, o campo LOCS inclui o ID do perfil de codificação de eliminação e o ID do grupo de codificação de eliminação

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contêiner e objeto do Swift, dependendo de qual API foi usada.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transações de exclusão de objetos

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de exclusão são incluídas.

Mensagens de auditoria de exclusão do S3

Código	Nome	Descrição	Rastro	Ver
SDEL	S3 Excluir	Solicitação feita para excluir o objeto de um bucket.	CBDI, S3KY	"SDEL: S3 EXCLUIR"

Mensagens de auditoria de exclusão rápida

Código	Nome	Descrição	Rastro	Ver
WDEL	Exclusão rápida	Solicitação feita para excluir o objeto de um contêiner, ou o contêiner.	CBDI, WOBJ	"WDEL: Swift EXCLUIR"

Exemplo: exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

> Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de exclusão do S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objetos começa quando o cliente envia uma solicitação DeleteObject para um serviço LDR. A mensagem contém o bucket do qual o objeto deve ser excluído e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transações de recuperação de objetos

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de recuperação são incluídas.

Mensagens de auditoria de recuperação S3

Código	Nome	Descrição	Rastro	Ver
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBDI, S3BK, S3KY	"SGET: S3 OBTER"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Rastro	Ver
WGET	Rápido GET	Solicitação feita para recuperar um objeto de um contêiner.	CBDI, WCON, WOBJ	"WGET: GET rápido"

Exemplo: recuperação de objeto S3

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de recuperação S3 (SGET) são listados.

SGET: S3 OBTER

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject para um serviço LDR. A mensagem contém o bucket do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política do bucket permitir, um cliente poderá recuperar objetos anonimamente ou recuperar objetos de um bucket que pertence a uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta do locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma solicitação GetObject para um objeto armazenado em um bucket que não é dele. Os valores para SBAI e SBAC registram o ID e o nome da conta do locatário do proprietário do bucket, que diferem do ID e do nome da conta do locatário do cliente registrados no S3AI e no SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemplo: S3 Select em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação S3 Select (SelectObjectContent) são listados.

Cada consulta resulta em duas mensagens de auditoria: uma que executa a autorização da solicitação S3 Select (o campo S3SR é definido como "select") e uma operação GET padrão subsequente que recupera os dados do armazenamento durante o processamento.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensagens de atualização de metadados

Mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados S3

Código	Nome	Descrição	Rastro	Ver
SUPD	Metadados S3 atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBDI, S3KY, HTRH	"SUPD: Metadados S3 atualizados"

Exemplo: atualização de metadados S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: Atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados(`x-amz-meta-\*`) para o objeto S3 (S3KY). Neste exemplo, os cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**). Ver "Configurar mensagens de auditoria e destinos de log" .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Mensagens de auditoria

Descrições de mensagens de auditoria

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema estão listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiro em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades que são auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas em ordem alfabética por seus códigos de quatro caracteres. Esta lista alfabética permite que você encontre informações sobre mensagens específicas.

Os códigos de quatro caracteres usados neste capítulo são os valores ATYP encontrados nas mensagens de auditoria, conforme mostrado na seguinte mensagem de exemplo:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Para obter informações sobre como definir níveis de mensagens de auditoria, alterar destinos de log e usar um servidor syslog externo para suas informações de auditoria, consulte"Configurar mensagens de auditoria e

destinos de log"

Categorias de mensagens de auditoria

Mensagens de auditoria do sistema

As mensagens de auditoria pertencentes à categoria de auditoria do sistema são usadas para eventos relacionados ao próprio sistema de auditoria, estados de nós de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Ver
ECMC	Fragmento de dados codificado por apagamento ausente: indica que um fragmento de dados codificado por apagamento ausente foi detectado.	"ECMC: Fragmento de dados codificado por apagamento ausente"
CEC	Fragmento de dados corrompido com codificação de eliminação: indica que um fragmento de dados corrompido com codificação de eliminação foi detectado.	"ECOC: Fragmento de dados codificados por apagamento corrompidos"
ETAF	Falha na autenticação de segurança: uma tentativa de conexão usando o Transport Layer Security (TLS) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .	"GNRG: Registro GNDS"
GNUR	Cancelamento de registro do GNDS: um serviço cancelou seu registro no sistema StorageGRID .	"GNUR: Cancelamento de registro do GNDS"
GTED	Tarefa de grade encerrada: o serviço CMN concluiu o processamento da tarefa de grade.	"GTED: Tarefa de grade encerrada"
GTST	Tarefa de grade iniciada: o serviço CMN começou a processar a tarefa de grade.	"GTST: Tarefa de grade iniciada"
GTSU	Tarefa de grade enviada: uma tarefa de grade foi enviada ao serviço CMN.	"GTSU: Tarefa de grade enviada"
LLST	Localização perdida: esta mensagem de auditoria é gerada quando uma localização é perdida.	"LLST: Localização Perdida"
OLST	Objeto perdido: um objeto solicitado não pode ser localizado no sistema StorageGRID .	"OLST: Sistema detectou objeto perdido"

Código	Título e descrição da mensagem	Ver
SADD	Desativar auditoria de segurança: o registro de mensagens de auditoria foi desativado.	"SADD: Desativação de auditoria de segurança"
SADE	Habilitar auditoria de segurança: o registro de mensagens de auditoria foi restaurado.	"SADE: Habilitar Auditoria de Segurança"
SVRF	Falha na verificação do Object Store: um bloco de conteúdo falhou nas verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
SVRU	Object Store Verify Unknown: Dados de objeto inesperados detectados no armazenamento de objetos.	"SVRU: Verificação de armazenamento de objeto desconhecido"
SYSD	Parada do nó: um desligamento foi solicitado.	"SYSD: Parada do nó"
SISTEMA	Parada de nó: um serviço iniciou uma parada normal.	"SYST: Parada do nó"
SYSU	Início do nó: um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: Início do nó"

Mensagens de auditoria de armazenamento de objetos

As mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos são usadas para eventos relacionados ao armazenamento e gerenciamento de objetos dentro do sistema StorageGRID . Isso inclui armazenamento e recuperação de objetos, transferências de nó de grade para nó de grade e verificações.

> Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Mensagens de auditoria de armazenamento de objetos do StorageGRID 11.8" .

Código	Descrição	Ver
IRMÃO	Solicitação de somente leitura de bucket: um bucket entrou ou saiu do modo somente leitura.	"BROR: Solicitação de somente leitura do bucket"
CBSE	Fim do envio do objeto: a entidade de origem concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBSE: Fim do envio de objeto"

Código	Descrição	Ver
CBRE	Fim do recebimento do objeto: a entidade de destino concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBRE: Objeto Recebimento Final"
CGRR	Solicitação de replicação entre grades: o StorageGRID tentou uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.	"CGRR: Solicitação de replicação entre redes"
EBDL	Exclusão de bucket vazio: o scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).	"EBDL: Exclusão de Bucket Vazio"
EBKR	Solicitação de bucket vazio: um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).	"EBKR: Solicitação de balde vazio"
SCMT	Confirmação do armazenamento de objetos: um bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado.	"SCMT: Solicitação de confirmação de armazenamento de objeto"
SREM	Remoção do Object Store: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Remoção de armazenamento de objetos"

O cliente leu mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Ver
S3SL	Solicitação S3 Select: Registra uma conclusão depois que uma solicitação S3 Select é retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.	Cliente S3	"S3SL: Solicitação de seleção S3"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 OBTER"

Código	Descrição	Usado por	Ver
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: CABEÇA S3"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	Cliente Swift	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	Cliente Swift	"WHEA: CABEÇA Rápida"

O cliente escreve mensagens de auditoria

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Ver
OVWR	Substituição de objeto: registra uma transação para substituir um objeto por outro objeto.	Clientes S3 e Swift	"OVWR: Substituição de Objeto"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 EXCLUIR"
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	"SPOS: POSTAGEM S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	Metadados S3 atualizados: registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	"SUPD: Metadados S3 atualizados"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	Cliente Swift	"WDEL: Swift EXCLUIR"

Código	Descrição	Usado por	Ver
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	Cliente Swift	"WPUT: PUT rápido"

Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento.

Código	Título e descrição da mensagem	Ver
MGAU	Mensagem de auditoria da API de gerenciamento: um log de solicitações do usuário.	"MGAU: Mensagem de auditoria de gestão"

Mensagens de auditoria do ILM

As mensagens de auditoria pertencentes à categoria de auditoria ILM são usadas para eventos relacionados às operações de gerenciamento do ciclo de vida da informação (ILM).

Código	Título e descrição da mensagem	Ver
IDEL	Exclusão iniciada pelo ILM: esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
LKCU	Limpeza de objetos sobrescritos. Esta mensagem de auditoria é gerada quando um objeto substituído é removido automaticamente para liberar espaço de armazenamento.	"LKCU: Limpeza de Objetos Sobrescritos"
ORLM	Regras de objeto atendidas: esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras do ILM.	"ORLM: Regras de Objeto Atendidas"

Referência de mensagem de auditoria

BROR: Solicitação de somente leitura do bucket

O serviço LDR gera esta mensagem de auditoria quando um bucket entra ou sai do modo somente leitura. Por exemplo, um bucket entra no modo somente leitura enquanto todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do balde	O ID do bucket.

Código	Campo	Descrição
IRMÃO	Valor de solicitação somente leitura do bucket	Se o bucket está se tornando somente leitura ou está saindo do estado somente leitura (1 = somente leitura, 0 = não somente leitura).
MANOS	Motivo de somente leitura do bucket	O motivo pelo qual o bucket está se tornando somente leitura ou saindo do estado somente leitura. Por exemplo, emptyBucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

CBRB: Início do recebimento do objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.

Código	Campo	Descrição
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBRE: Objeto Recebimento Final

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.

Código	Campo	Descrição
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBSE: Fim do envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: Transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CGRR: Solicitação de replicação entre redes

Esta mensagem é gerada quando o StorageGRID tenta uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de

grade.

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes. O atributo CSIZ foi introduzido no StorageGRID 11.8. Como resultado, as solicitações de replicação entre grades abrangendo uma atualização do StorageGRID 11.7 para 11.8 podem ter um tamanho total de objeto impreciso.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que possui o bucket do qual o objeto está sendo replicado.
GFID	ID de conexão da federação de grade	O ID da conexão de federação de grade que está sendo usada para replicação entre grades.
OPER	Operação CGR	O tipo de operação de replicação entre grades que foi tentada: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de exclusão
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.
VSID	ID da versão	O ID da versão específica de um objeto que estava sendo replicado.
RSLT	Código de resultado	Retorna erro bem-sucedido (SUCS) ou erro geral (GERR).

EBDL: Exclusão de Bucket Vazio

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.

Código	Campo	Descrição
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
RSLT	Resultado da operação de exclusão	O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é usado em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

EBKR: Solicitação de balde vazio

Esta mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).

Código	Campo	Descrição
CONSTRUIR	UUID do balde	O ID do bucket.
EBJS	Configuração JSON do Bucket Vazio	Contém o JSON que representa a configuração atual do Empty Bucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

ECMC: Fragmento de dados codificado por apagamento ausente

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados codificado para eliminação ausente.

Código	Campo	Descrição
VCMC	ID do VCS	O nome do VCS que contém o pedaço faltante.
MCID	ID do pedaço	O identificador do fragmento codificado por apagamento ausente.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificados por apagamento corrompidos

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados corrompido com código de eliminação.

Código	Campo	Descrição
VCCO	ID do VCS	O nome do VCS que contém o pedaço corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido com código de eliminação.
CCID	ID do pedaço	O identificador do fragmento corrompido codificado por apagamento.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando o Transport Layer Security (TLS) falha.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP na qual a autenticação falhou.
RUID	Identidade do usuário	Um identificador dependente de serviço que representa a identidade do usuário remoto.
RSLT	Código de Razão	O motivo da falha: SCNI: Falha no estabelecimento da conexão segura. CERM: O certificado estava faltando. CERT: O certificado era inválido. CERE: O certificado expirou. CERR: O certificado foi revogado. CSGN: A assinatura do certificado era inválida. CSGU: O signatário do certificado era desconhecido. UCRM: As credenciais do usuário estavam faltando. UCRI: As credenciais do usuário eram inválidas. UCRU: Credenciais de usuário não foram permitidas. TOUT: Tempo limite de autenticação esgotado.

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e lógica adicional incorporada ao serviço. Se essa autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, uma mensagem de auditoria será registrada. Isso permite consultas sobre tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota com configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Esta mensagem de auditoria deve ser monitorada para detectar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.
GNTP	Tipo de dispositivo	O tipo de dispositivo do nó da grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A sequência de caracteres que identifica a versão do modelo do dispositivo do nó da grade no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consulta de serviço).
GNIA	Endereço IP	Endereço IP do nó da grade.

Esta mensagem é gerada sempre que um nó de grade atualiza sua entrada no Pacote de Nós de Grade.

GNUR: Cancelamento de registro do GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço possui informações não registradas sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grade encerrada

Esta mensagem de auditoria indica que o serviço CMN concluiu o processamento da tarefa de grade especificada e moveu a tarefa para a tabela Histórica. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria correspondente de Tarefa de grade iniciada. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa de grade seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
RSLT	Resultado	O resultado final do status da tarefa de grade: • SUCS: A tarefa da grade foi concluída com sucesso. • ABRT: A tarefa da grade foi encerrada sem erro de reversão. • ROLF: A tarefa da grade foi encerrada e não foi possível concluir o processo de reversão. • CANC: A tarefa da grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como duplicada.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem Grid Task Submitted para tarefas de grade iniciadas pelo serviço interno Grid Task Submission e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela Pendente, esta mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
RSLT	Resultado	O resultado. Este campo tem apenas um valor: • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grade enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	ID da tarefa	Identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
TTYP	Tipo de tarefa	O tipo de tarefa de grade.
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição da tarefa	Uma descrição legível da tarefa da grade.

Código	Campo	Descrição
IVA	Válido após o carimbo de data/hora	O primeiro momento (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do carimbo de data/hora	O horário mais recente (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A fonte da tarefa: • TXTB: A tarefa de grade foi enviada por meio do sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada por meio do Serviço de Envio de Tarefas de Grade interno.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi enviada para ativação automática. • PEND: A tarefa da grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.
RSLT	Resultado	O resultado da submissão: • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: Exclusão iniciada pelo ILM

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis**: Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis**. Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento nas políticas ativas do ILM se aplica atualmente ao objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.

Código	Campo	Descrição
APLV	Conformidade: Exclusão automática	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o bucket esteja sob retenção legal.
CMPL	Conformidade: retenção legal	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se o bucket está atualmente sob retenção legal.
CMPR	Conformidade: Período de retenção	Somente para objetos em buckets S3 compatíveis. A duração do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Somente para objetos em buckets S3 compatíveis. Tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do bucket.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.

Código	Campo	Descrição
REGRA	Etiqueta de regras	• Se um objeto em um bucket S3 compatível estiver sendo excluído automaticamente porque seu período de retenção expirou, este campo ficará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se apliquem atualmente ao objeto, este campo mostrará o rótulo legível da última regra do ILM aplicada ao objeto.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

LKCU: Limpeza de Objetos Sobrescritos

Esta mensagem é gerada quando o StorageGRID remove um objeto substituído que anteriormente exigia limpeza para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	*Somente para uso interno.*
LUID	UUID do objeto removido	O identificador do objeto que foi removido.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
UUID	Identificador Universalmente Único	O identificador do objeto que ainda existe. Este valor só estará disponível se o objeto não tiver sido excluído.

LKDM: Limpeza de Objetos Vazados

Esta mensagem é gerada quando um pedaço vazado é limpo ou excluído. Um pedaço pode ser parte de um objeto replicado ou de um objeto codificado para eliminação.

Código	Campo	Descrição
CLOC	Localização do pedaço	O caminho do arquivo do pedaço vazado que foi excluído.

CTYP	Tipo de pedaço	Tipo de pedaço:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	Tipo de vazamento	Os cinco tipos de vazamentos que podem ser detectados:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Tempo de criação do bloco	Horário em que o pedaço vazado foi criado.
UUID	Identificador Universalmente Único	O identificador do objeto ao qual o pedaço pertence.
CBDI	Identificador de bloco de conteúdo	CBID do objeto ao qual o pedaço vazado pertence.
CSIZ	Tamanho do conteúdo	O tamanho do pedaço em bytes.

LLST: Localização Perdida

Esta mensagem é gerada sempre que um local para uma cópia de objeto (replicada ou

codificada para eliminação) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBDI	O CBDI afetado.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por eliminação. O ID do perfil de codificação de eliminação usado.
LTYP	Tipo de localização	CLDI (Online): Para dados de objetos replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
NOID	ID do nó de origem	O ID do nó no qual os locais foram perdidos.
PCLD	Caminho para o objeto replicado	O caminho completo para o local do disco dos dados do objeto perdido. Retornado somente quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Assume a forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Resultado	Sempre NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de disparo	USUÁRIO: Acionado pelo usuário SYST: Sistema acionado
UUID	ID universalmente exclusivo	O identificador do objeto afetado no sistema StorageGRID .

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento. Cada solicitação HTTP que não é uma solicitação GET ou HEAD para um URI de API válido registra uma resposta contendo o nome de usuário, IP e tipo de solicitação para a API. URIs de API inválidos (como /api/v3-authorize) e solicitações inválidas para URIs de API válidos não são registrados.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome do domínio do host.
MPAT	Solicitar PATH	O caminho da solicitação.
MPQP	Parâmetros de consulta de solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo da solicitação	O conteúdo do corpo da solicitação. Embora o corpo da resposta seja registrado por padrão, o corpo da solicitação é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo da resposta, elas são obtidas do corpo da solicitação para os seguintes métodos POST: • Nome de usuário e ID da conta em **POST autorizar** • Nova configuração de sub-redes em **POST /grid/grid-networks/update** • Novos servidores NTP em **POST /grid/ntp-servers/update** • IDs de servidores desativados em **POST /grid/servers/decommission** **Observação:** Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MRMD	Método de solicitação	O método de solicitação HTTP: • PUBLICAR • COLOCAR • EXCLUIR • CORREÇÃO
MRSC	Código de resposta	O código de resposta.
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. **Observação:** Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).

Código	Campo	Descrição
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN do usuário	O URN (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna sucesso (SUCS) ou o erro relatado pelo backend.

OLST: Sistema detectou objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar nenhuma cópia de um objeto no sistema StorageGRID .

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto perdido.
NOID	ID do nó	Se disponível, a última localização direta ou próxima conhecida do objeto perdido. É possível ter apenas o ID do nó sem um ID do volume se as informações do volume não estiverem disponíveis.
CAMINHO	Balde/Chave S3	Se disponível, o nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
UUID	ID universalmente exclusivo	O identificador do objeto perdido dentro do sistema StorageGRID .
VOLI	ID do volume	Se disponível, o ID do volume do nó de armazenamento para o último local conhecido do objeto perdido.

ORLM: Regras de Objeto Atendidas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras do ILM.

> ⓘ A mensagem ORLM não é gerada quando um objeto é armazenado com sucesso pela regra padrão Fazer 2 Cópias se outra regra na política usar o filtro avançado Tamanho do Objeto.

Código	Campo	Descrição
CONSTRUIR	Cabeçalho de balde	Campo ID do bucket. Usado para operações internas. Aparece somente se STAT for PRGD.
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível dado à regra ILM aplicada a este objeto.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
SGCB	CBDID do contêiner	CBID do contêiner para o objeto segmentado. Este valor está disponível somente para objetos segmentados e multipartes.

Código	Campo	Descrição
ESTATÍSTICA	Status	O status da operação do ILM. CONCLUÍDO: As operações do ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação do ILM. PRGD: O objeto foi excluído do sistema StorageGRID . NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID . Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

A mensagem de auditoria ORLM pode ser emitida mais de uma vez para um único objeto. Por exemplo, ele é emitido sempre que ocorre um dos seguintes eventos:

- As regras do ILM para o objeto são satisfeitas para sempre.
- As regras do ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano detecta que uma cópia dos dados do objeto replicado está corrompida. O sistema StorageGRID executa uma avaliação do ILM para substituir o objeto corrompido.

Informações relacionadas

- "Transações de ingestão de objetos"
- "Transações de exclusão de objetos"

OVWR: Substituição de Objeto

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo (novo)	O CBDID para o novo objeto.
CSIZ	Tamanho do objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.

Código	Campo	Descrição
TOCB	Identificador de bloco de conteúdo (anterior)	O CBDID do objeto anterior.
UUID	ID universalmente exclusivo (novo)	O identificador do novo objeto dentro do sistema StorageGRID .
OUID	ID universalmente exclusivo (anterior)	O identificador do objeto anterior dentro do sistema StorageGRID .
CAMINHO	Caminho do objeto S3	O caminho do objeto S3 usado para o objeto anterior e o novo
RSLT	Código de resultado	Resultado da transação de substituição de objeto. O resultado é sempre: SUCS: Bem-sucedido
SGRP	Site (Grupo)	Se presente, o objeto substituído foi excluído no site especificado, que não é o site onde o objeto substituído foi ingerido.

S3SL: Solicitação de seleção S3

Esta mensagem registra uma conclusão após uma solicitação S3 Select ter sido retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.

Código	Campo	Descrição
BYSC	Bytes escaneados	Número de bytes escaneados (recebidos) dos nós de armazenamento. BYSC e BYPR provavelmente serão diferentes se o objeto for compactado. Se o objeto for compactado, BYSC terá a contagem de bytes compactados e BYPR serão os bytes após a descompactação.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "Bytes escaneados" foram realmente processados ou acionados por um trabalho S3 Select.
BYRT	Bytes retornados	Número de bytes que um trabalho S3 Select retornou ao cliente.
REPR	Registros processados	Número de registros ou linhas que um trabalho S3 Select recebeu dos nós de armazenamento.

Código	Campo	Descrição
RERT	Registros Retornados	Número de registros ou linhas que um trabalho do S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se o trabalho S3 Select concluiu o processamento ou não. Se isso for falso, o trabalho não foi concluído e os campos de erro provavelmente conterão dados. O cliente pode ter recebido resultados parciais ou nenhum resultado.
REID	ID da solicitação	Identificador para a solicitação S3 Select.
EXTM	Tempo de execução	O tempo, em segundos, que levou para o S3 Select Job ser concluído.
ERMG	Mensagem de erro	Mensagem de erro gerada pelo trabalho S3 Select.
ERTY	Tipo de erro	Tipo de erro gerado pelo trabalho S3 Select.
ERST	Rastreamento de pilha de erros	Rastreamento de pilha de erros gerado pelo trabalho S3 Select.
S3BK	Balde S3	O nome do bucket S3.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 para o usuário que enviou a solicitação.
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.

SADD: Desativação de auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) desativou o registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para desabilitar a auditoria.

Código	Campo	Descrição
AEUN	Nome de usuário	O nome de usuário que executou o comando para desabilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro estava habilitado anteriormente, mas agora foi desabilitado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SADE: Habilitar Auditoria de Segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registro de mensagens de auditoria; as mensagens de auditoria estão sendo coletadas e entregues novamente.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para permitir a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para habilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro foi desabilitado anteriormente (SADD), mas agora foi restaurado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SCMT: Confirmação do Armazenamento de Objetos

O conteúdo da grade não é disponibilizado nem reconhecido como armazenado até que tenha sido confirmado (o que significa que foi armazenado persistentemente). O conteúdo armazenado de forma persistente foi completamente gravado no disco e passou pelas verificações de integridade relacionadas. Esta mensagem é emitida quando um bloco de conteúdo é confirmado no armazenamento.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com armazenamento permanente.
RSLT	Código de resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 EXCLUIR

Quando um cliente S3 emite uma transação DELETE, uma solicitação é feita para remover o objeto ou bucket especificado, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em buckets não incluem este campo.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `x-amz-bypass-governance-retention`é incluído automaticamente se estiver presente na solicitação.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUDM	Identificador universalmente exclusivo para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens do log de auditoria especificam UUDM ou UUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto, e UUID indica um objeto.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 OBTER

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LIDADE	ListObjectsV2	Uma resposta no formato *v2* foi solicitada. Para mais detalhes, veja "AWS ListObjectsV2" . Somente para operações de bucket GET.
NCHD	Número de filhos	Inclui chaves e prefixos comuns. Somente para operações de bucket GET.
ALCANCE	Leitura de intervalo	Somente para operações de leitura de intervalo. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho do objeto inteiro.
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.

Código	Campo	Descrição
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.

Código	Campo	Descrição
TRNC	Truncado ou Não Truncado	Defina como falso se todos os resultados foram retornados. Defina como verdadeiro se houver mais resultados disponíveis para retornar. Somente para operações de bucket GET.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: CABEÇA S3

Quando um cliente S3 emite uma transação HEAD, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.

Código	Campo	Descrição
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: POSTAGEM S3

Quando um cliente S3 emite uma solicitação de objeto POST, esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `` (Não esperado para SPOS).
RSLT	Código de resultado	Resultado da solicitação RestoreObject. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável. Defina como "selecionar" para uma operação S3 Select.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	Restaurar informações.

Código	Campo	Descrição
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CMPS	Configurações de conformidade	As configurações de conformidade usadas ao criar o bucket, se presentes na solicitação (truncadas para os primeiros 1024 caracteres).
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.

Código	Campo	Descrição
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `x-amz-bypass-governance-retention`é incluído automaticamente se estiver presente na solicitação.
LKEN	Bloqueio de objeto habilitado	Valor do cabeçalho da solicitação `x-amz-bucket-object-lock-enabled` , se presente na solicitação.
LKLH	Bloqueio de objeto - retenção legal	Valor do cabeçalho da solicitação `x-amz-object-lock-legal-hold` , se presente na solicitação PutObject.
LKMD	Modo de retenção de bloqueio de objeto	Valor do cabeçalho da solicitação `x-amz-object-lock-mode` , se presente na solicitação PutObject.
LKRU	Bloqueio de objeto reter até a data	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date` , se presente na solicitação PutObject. Os valores são limitados a 100 anos a partir da data em que o objeto foi ingerido.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	A nova configuração de sub-recursos (truncada para os primeiros 1024 caracteres).
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.

Código	Campo	Descrição
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
ULID	ID de upload	Incluído somente em mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as peças foram carregadas e montadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "habilitado" ou "suspenso". Operações em objetos não incluem este campo.

SREM: Remoção de armazenamento de objetos

Esta mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não está mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código de resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Esta mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

SUPD: Metadados S3 atualizados

Esta mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização de metadados for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SVRF: Falha na verificação do armazenamento de objetos

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que dados de objetos replicados são lidos ou gravados no disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente inseridos no sistema. Se alguma dessas verificações falhar, o sistema colocará automaticamente

em quarentena os dados corrompidos do objeto replicado para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou na verificação.
RSLT	Código de resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação do código de autenticação de mensagem baseado em hash (HMAC). EHSH: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. PERR: Estrutura inválida do arquivo de disco. DERR: Erro de disco. FNAM: Nome de arquivo incorreto.

Esta mensagem deve ser monitorada de perto. Falhas na verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar qual operação acionou a mensagem, consulte o valor do campo AMID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano, e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação de armazenamento de objeto desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detectada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do arquivo	O caminho do arquivo da cópia inesperada do objeto.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

A mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objeto foram detectadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, essa mensagem é enviada somente após uma reinicialização subsequente, porque a fila de mensagens de auditoria não é limpa antes do desligamento. Procure a mensagem SYST, enviada no início da sequência de desligamento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYST: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. SYST pode ser usado para determinar se o desligamento foi solicitado antes do serviço ser reiniciado (ao contrário de SYSD, que normalmente é enviado após a reinicialização do serviço).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem SYST não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, esta mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (já que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Gerenciador do Servidor reinicia automaticamente um serviço com falha.

WDEL: Swift EXCLUIR

Quando um cliente Swift emite uma transação DELETE, uma solicitação é feita para remover o objeto ou contêiner especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WGET: GET rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contêiner ou listar os contêineres em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA Rápida

Quando um cliente Swift emite uma transação HEAD, uma solicitação é feita para verificar a existência de uma conta, contêiner ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código de resultado	Resultado da transação HEAD. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: PUT rápido

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contêiner. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .

Código	Campo	Descrição
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

Informações sobre direitos autorais

Informações sobre marcas comerciais