Monitorar e solucionar problemas

StorageGRID

NetApp
December 03, 2025

Índice

Monitore e solucione problemas de um sistema StorageGRID

Monitore o sistema StorageGRID

Monitorar um sistema StorageGRID: Visão geral

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

Antes de começar

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

> Para alterar unidades para os valores de armazenamento exibidos no Gerenciador de Grade, selecione o usuário suspenso no canto superior direito do Gerenciador de Grade e selecione **Preferências do usuário**.

Sobre esta tarefa

Estas instruções descrevem como:

- "Visualizar e gerenciar o painel"
- "Exibir a página nós"
- "Monitorize estes aspetos do sistema regularmente:"
  - "Integridade do sistema"
  - "Capacidade de storage"
  - "Gerenciamento do ciclo de vida das informações"
  - "Recursos de rede e sistema"
  - "Atividade do locatário"
  - "Operações de balanceamento de carga"
  - "Conexões de federação de grade"
  - "Capacidade de arquivamento"
- "Gerencie alertas e alarmes legados"
- "Ver ficheiros de registo"
- "Configurar mensagens de auditoria e destinos de log"
- "Use um servidor syslog externo" para coletar informações de auditoria
- "Utilize SNMP para monitorização"
- "Obter dados StorageGRID adicionais", incluindo métricas e diagnósticos

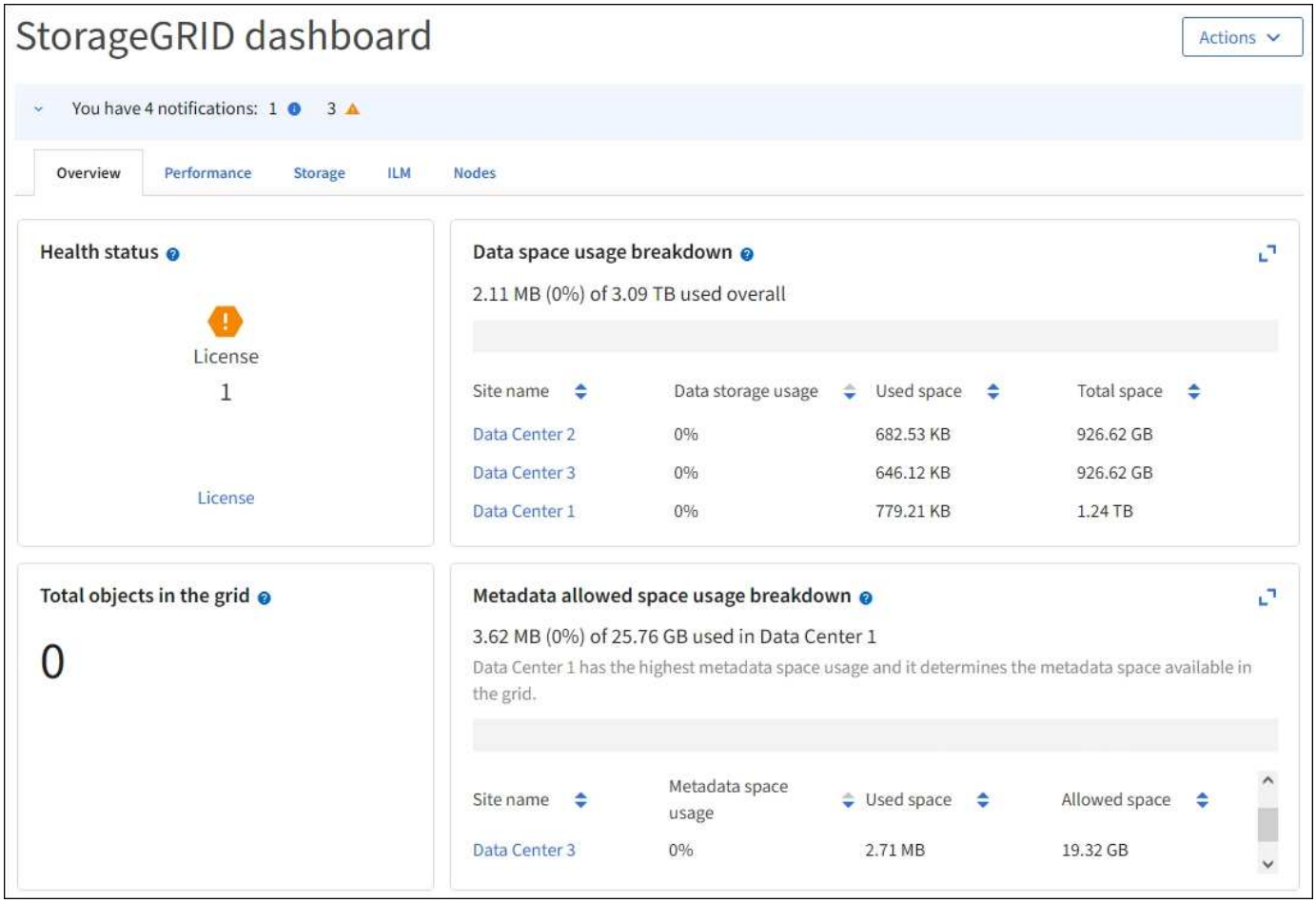
Visualizar e gerenciar o painel

Você pode usar o painel para monitorar rapidamente as atividades do sistema. Você

pode criar painéis personalizados para monitorar a implementação do StorageGRID.

Para alterar unidades para os valores de armazenamento exibidos no Gerenciador de Grade, selecione o usuário suspenso no canto superior direito do Gerenciador de Grade e selecione **Preferências do usuário**.

Seu painel pode ser diferente com base na configuração do sistema.



Visualizar o painel de instrumentos

O painel é composto por separadores que contêm informações específicas sobre o sistema StorageGRID. Cada guia 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 contêm apenas as guias e cartões relevantes para o monitoramento da implementação do StorageGRID.

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

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

Separador no painel de instrumentos fornecido pelo sistema	Contém
Desempenho	Uso de espaço, armazenamento usado ao longo do tempo, operações S3 ou Swift, duração da solicitação, taxa de erro.
Armazenamento	Uso da cota de locatário e uso do espaço lógico. Previsões de uso de espaço para dados de usuário e metadados.
ILM	Fila de gerenciamento do ciclo de vida das informações e taxa de avaliação.
Nós	Uso de CPU, dados e memória por nó. S3 ou Swift operações por nó. Distribuição nó a local.

Alguns dos 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 minimizar ou selecione **Fechar**.

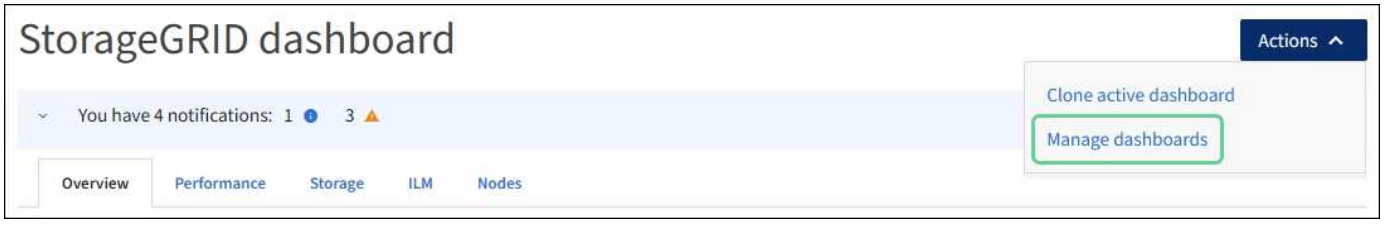
Gerenciar painéis

Se você tiver acesso root ("Permissões do grupo de administração"consulte), poderá 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.
- Clonar 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.
- Edite um nome de painel.
- Edite um painel para adicionar ou remover guias e cartões. Você pode ter um mínimo de 1 e um máximo de 20 guias.
- Retire um painel de bordo.

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

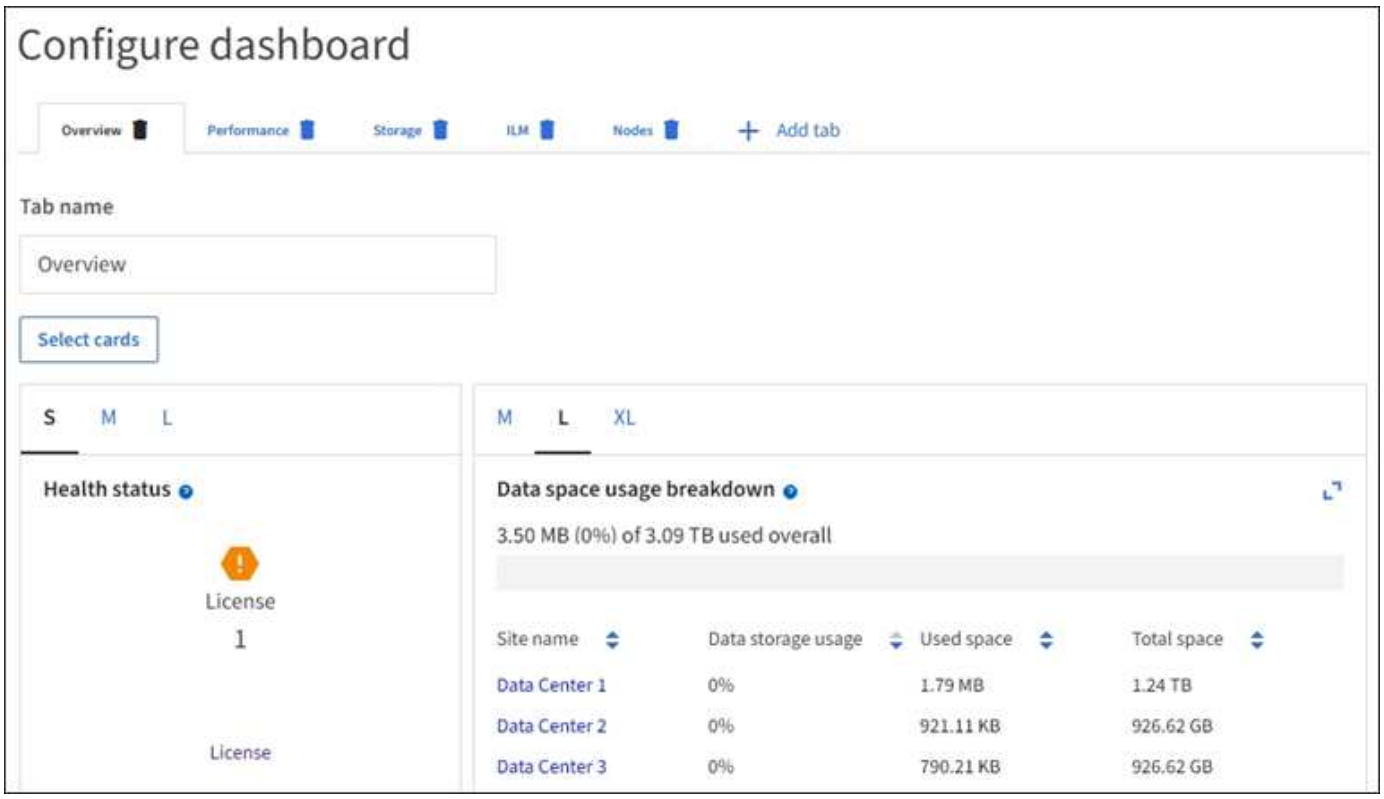
Para criar um novo painel clonando o painel ativo, selecione **ações** > **Clonar painel ativo**.

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 dashboard, você pode:

- Adicionar ou remover separadores
- Renomeie as guias e dê nomes exclusivos às novas guias
- Adicione, remova ou reorganize (arraste) cartões para cada guia
- Selecione o tamanho para cartões individuais selecionando **S**, **M**, **L** ou **XL** na parte superior do cartão



Exibir a página nós

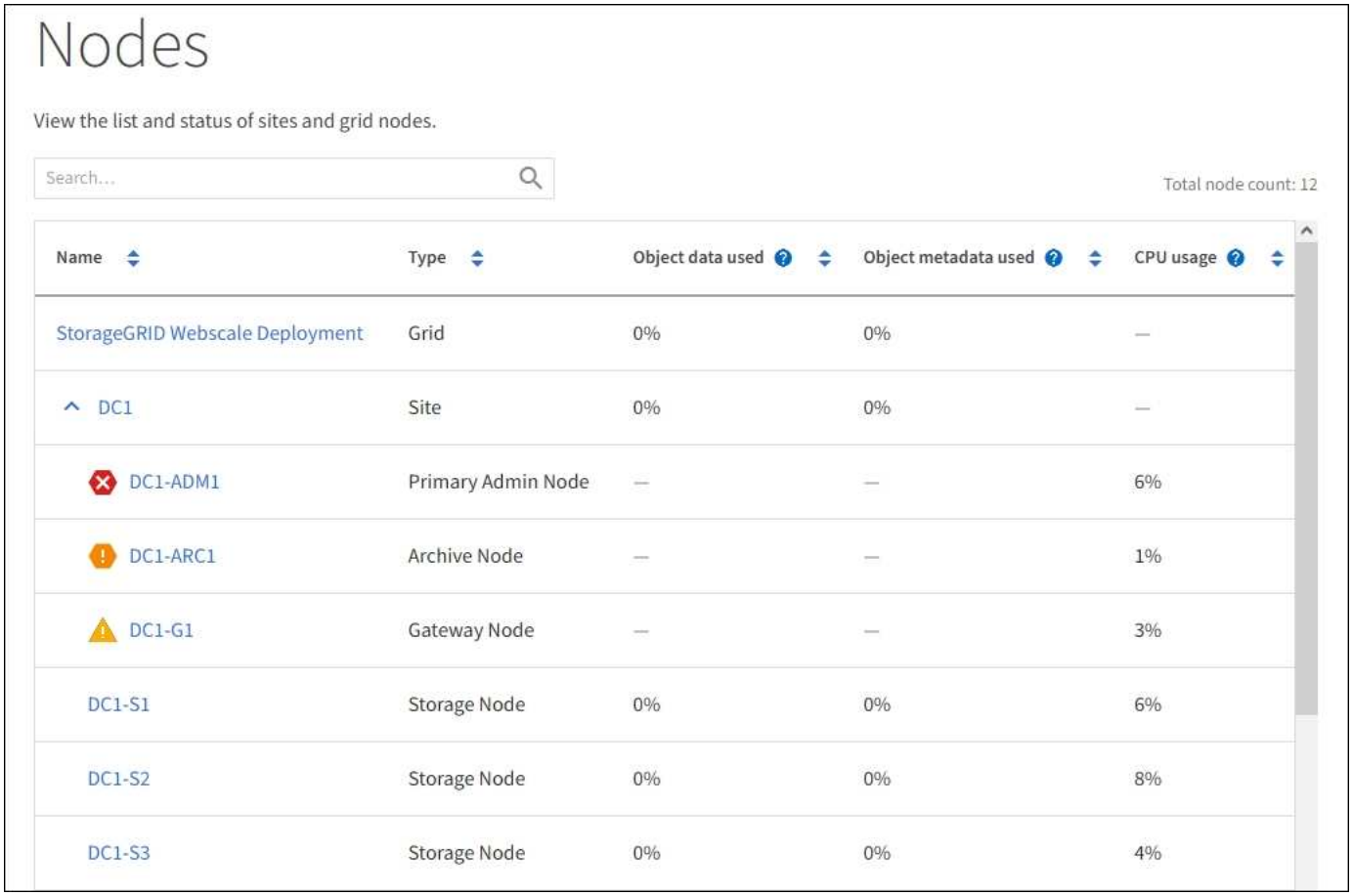
Exibir a página de nós: Visão geral

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

A tabela nós lista informações resumidas para toda a grade, cada local e cada nó. Se um nó estiver desconetado ou tiver um alerta ativo, um ícone será exibido ao lado do nome do nó. Se o nó estiver conetado e não tiver alertas ativos, nenhum ícone será exibido.

Quando um nó não está conetado à grade, como durante a atualização ou um estado desconetado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da grade. Depois que um nó se reconeta à grade, espere vários minutos para que os valores se estabilizem.

Para alterar unidades para os valores de armazenamento exibidos no Gerenciador de Grade, selecione o usuário suspenso no canto superior direito do Gerenciador de Grade e selecione **Preferências do usuário**.



Ícones de estado da ligação

Se um nó for desconetado da grade, um dos ícones a seguir será exibido ao lado do nome do nó.

Ícone	Descrição	Ação necessária
	**Não ligado - desconhecido** Por um motivo desconhecido, um nó é desconetado ou os serviços no nó estão inalterados inesperadamente. 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 é possível se 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 tenha parado ou reiniciado o host para o nó. **Nota**: Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.
	**Não conetado - administrativamente para baixo** Por um motivo esperado, o nó não está conetado à grade. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam online sem nenhuma intervenção.	Determine se algum alerta está afetando esse nó. Se um ou mais alertas estiverem ativos "Selecione cada alerta"e siga as ações recomendadas.

Se um nó for desconetado da grade, ele pode ter um alerta subjacente, mas somente o ícone "não conetado" será exibido. 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 será exibido ao lado do nome do nó:

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

 **Major**: 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 pare a operação normal de um nó ou serviço StorageGRID.

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

Exibir detalhes de um sistema, local ou nó

Para filtrar as informações mostradas na tabela nodes, insira uma cadeia de carateres de pesquisa no campo **Search**. Você pode pesquisar por nome do sistema, nome de exibição ou tipo (por exemplo, digite **Gat** para localizar rapidamente todos os nós do Gateway).

Para exibir as informações da grade, do local ou do nó:

- Selecione o nome da grade para ver um resumo agregado das estatísticas de todo o seu sistema StorageGRID.
- Selecione um local específico do data center para ver um resumo agregado das estatísticas de todos os nós nesse local.
- Selecione um nó específico para exibir informações detalhadas para esse nó.

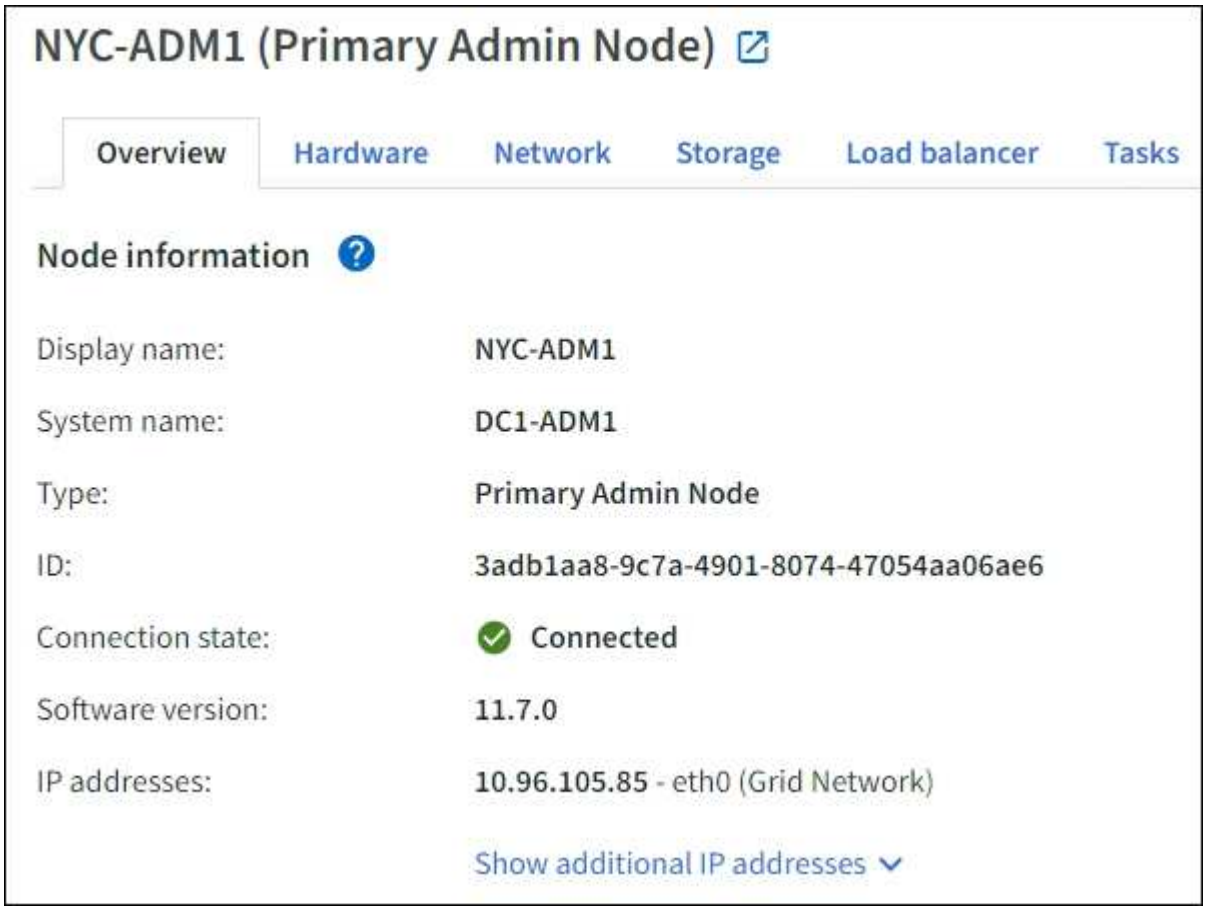
Veja a guia Visão geral

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

A guia Visão geral é mostrada para todos os nós.

Informações do nó

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



As informações de visão geral de um nó incluem o seguinte:

- **Nome de exibição** (mostrado somente se o nó tiver sido renomeado): O nome de exibição atual do nó. Utilize o "Renomeie 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 Admin, nó Admin primário, nó de armazenamento, nó de gateway ou nó de arquivo.

> O suporte para nós de arquivo está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade.

- **ID**: O identificador exclusivo para o nó, que também é conhecido como UUID.
- **Estado da conexão**: Um dos três estados. É apresentado o ícone para o estado mais grave.
  - **Desconhecido** : por um motivo desconhecido, o nó não está conetado à grade ou um ou mais serviços estão inalterados inesperadamente. Por exemplo, a conexão de rede entre nós foi perdida, a energia está inativa ou um serviço está inativo. O alerta **não é possível se 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. Nesses casos, você pode ignorar o estado desconhecido.

  - **Administrativamente para baixo** : o nó não está conetado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.
  - **Conectado** : o nó está conetado à grade.
- **Storage usado**: Somente para nós de storage.
  - **Dados do objeto**: A porcentagem do espaço utilizável total para dados de objeto que foram usados no nó de armazenamento.
  - **Metadados de objetos**: A porcentagem do espaço total permitido para metadados de objetos que foram usados no nó de armazenamento.
- **Versão do software**: A versão do StorageGRID instalada no nó.
- **Grupos de HA**: Somente para nó de administrador 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 principal.
- **Endereços IP**: Os endereços IP do nó. Clique em **Mostrar endereços IP adicionais** para visualizar os endereços IPv4 e IPv6 do nó e mapeamentos de interface.

Alertas

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

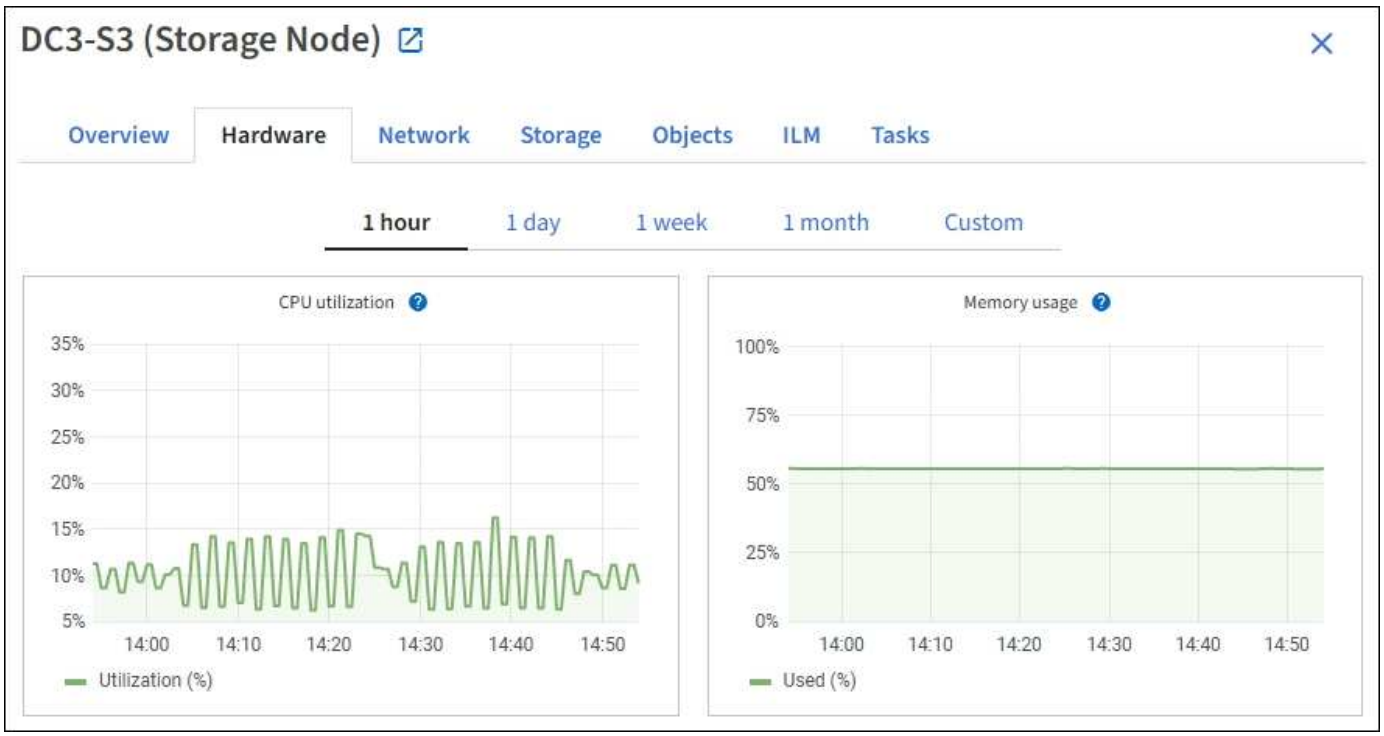
Os alertas também estão incluídos no "estados de conexão do nó".

Exibir a guia hardware

A guia hardware exibe a utilização da CPU e o uso da memória para cada nó e informações adicionais de hardware sobre dispositivos.

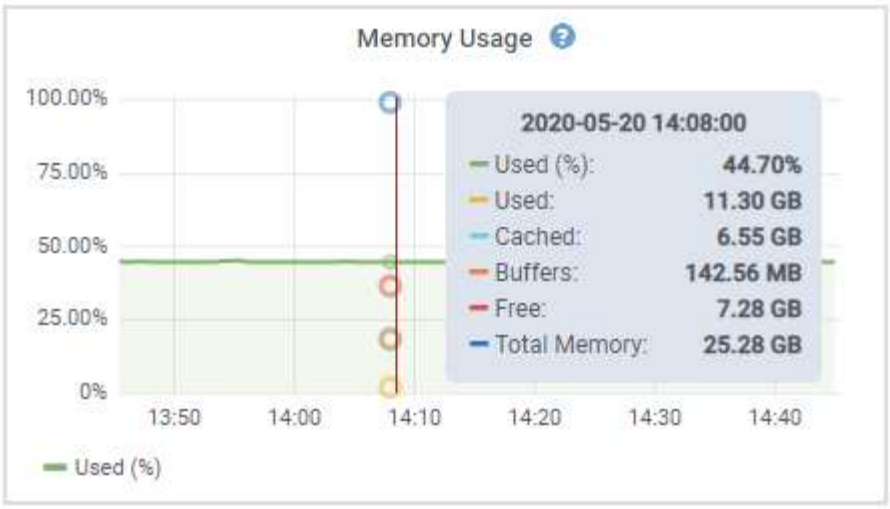
O Gerenciador de Grade é atualizado com cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A guia hardware é exibida para todos os nós.



Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou 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 o uso da memória, posicione o cursor sobre cada gráfico.



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

Exibir informações sobre os nós de storage do dispositivo

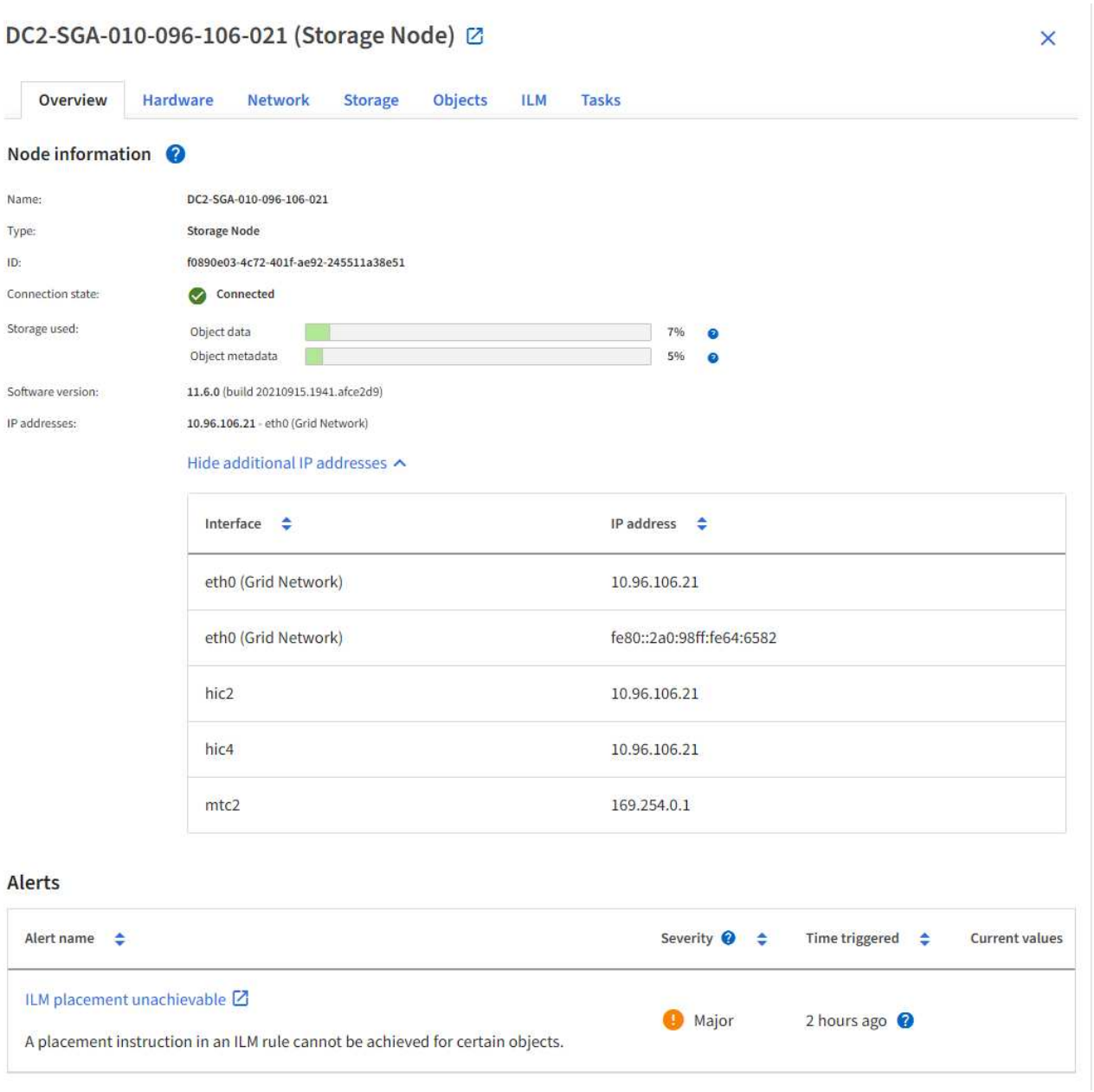
A página nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada nó de storage do dispositivo. Você também pode ver memória, hardware de armazenamento, versão do firmware do controlador, recursos de rede, interfaces de rede,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

Passos

1. Na página nós, selecione um nó de storage 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 do nó. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte forma:

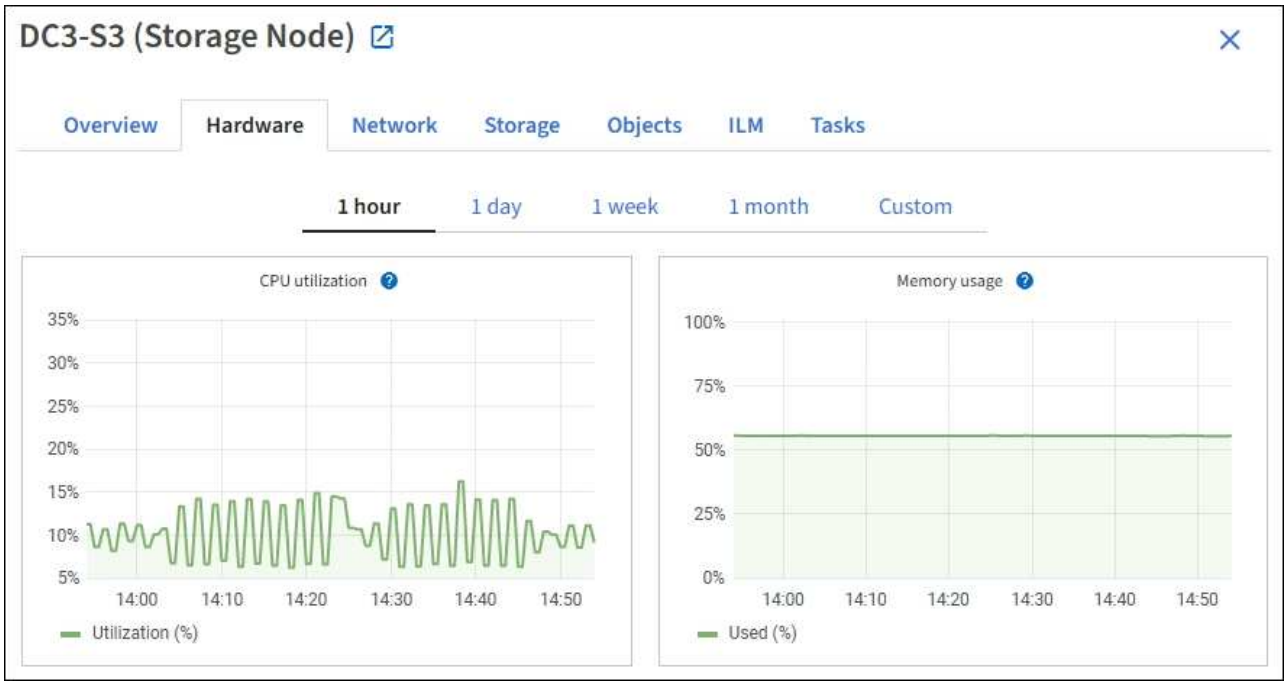
   - **eth**: Rede de Grade, rede Admin ou rede de cliente.
   - **Hic**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Estas portas podem ser Unidas e ligadas à rede de grelha StorageGRID (eth0) e à rede de clientes (eth2).
   - **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são ligadas para formar a interface de rede de administração do StorageGRID (eth1). Pode deixar outras interfaces mtc disponíveis para conetividade local temporária para um técnico no centro de dados.



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

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

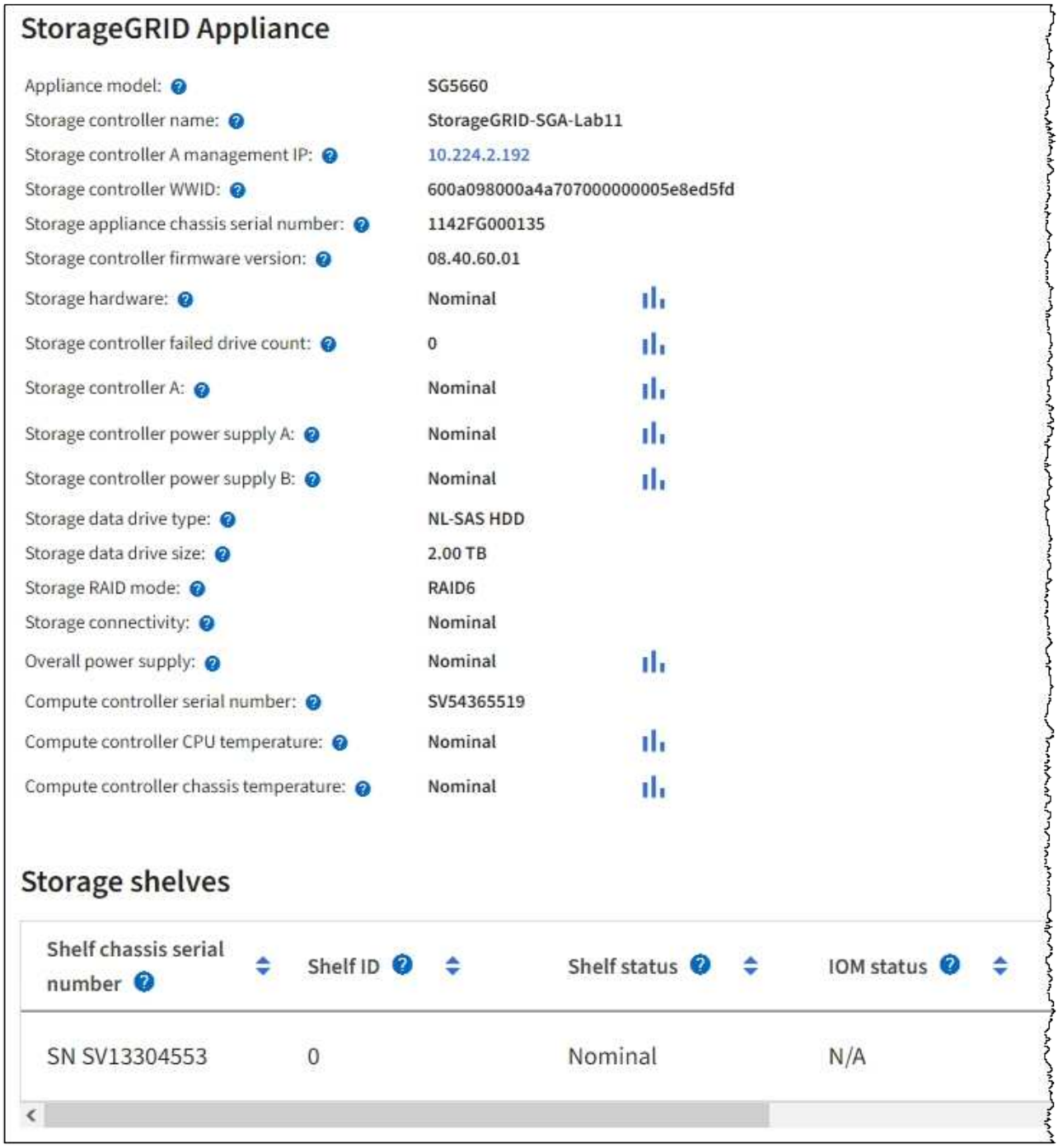
   a. Visualize os gráficos de utilização da CPU e memória para determinar as percentagens de utilização da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou gráfico. Você pode exibir as informações disponíveis para intervalos 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 aparelho; nomes do controlador, números de série e endereços IP; e o status de cada componente.

> Alguns campos, como o BMC IP do controlador de computação e o hardware de computação, aparecem apenas para dispositivos com esse recurso.

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



Campo na mesa do aparelho	Descrição
Modelo do aparelho	O número do modelo para este dispositivo StorageGRID mostrado no SANtricity os.
Nome do controlador de storage	O nome deste dispositivo StorageGRID mostrado no SANtricity os.
Um IP de gerenciamento do controlador de armazenamento	Endereço IP da porta de gerenciamento 1 no controlador de armazenamento A. você usa esse IP para acessar o SANtricity os para solucionar problemas de armazenamento.

Campo na mesa do aparelho	Descrição
IP de gerenciamento B do controlador de armazenamento	Endereço IP da porta de gerenciamento 1 no controlador de storage B. você usa esse IP para acessar o SANtricity os para solucionar problemas de storage. Alguns modelos de aparelhos não têm um controlador de armazenamento B..
Controlador de armazenamento WWID	O identificador mundial do controlador de storage mostrado no SANtricity os.
Número de série do chassi do dispositivo de armazenamento	O número de série do chassis do aparelho.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento para este dispositivo.
Hardware de storage	O status geral do hardware do controlador de storage. Se o Gerenciador de sistema do SANtricity relatar um status de precisa de atenção para o hardware de storage, o sistema StorageGRID também informará 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 existem outros alarmes que se apliquem ao controlador de computação.
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Controlador de Storage A	O status do controlador de armazenamento A..
Controlador de armazenamento B	O status do controlador de armazenamento B. alguns modelos de aparelhos não têm um controlador de armazenamento B.
Fonte de Alimentação do controlador de armazenamento A	O estado da fonte de Alimentação A para o controlador de armazenamento.
Fonte de alimentação B do controlador de armazenamento	O estado da fonte de alimentação B para o controlador de armazenamento.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).

Campo na mesa do aparelho	Descrição
Tamanho da unidade de dados de armazenamento	O tamanho efetivo de uma unidade de dados. **Nota**: Para nós com compartimentos de expansão, use o Tamanho da unidade de dados para cada gaveta em vez disso. O tamanho efetivo da unidade pode ser diferente por gaveta.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de storage	O estado de conetividade de storage.
Fonte de alimentação geral	O estado de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento de placa base (BMC) no controlador de computação. Você usa esse IP para se conetar à interface do BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é apresentado para modelos de aparelhos que não contêm um BMC.
Número de série do controlador de computação	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação. Esse campo não é exibido para modelos de dispositivo que não têm hardware de computação e hardware de armazenamento separados.
Temperatura da CPU do controlador de computação	O status da temperatura da CPU do controlador de computação.
Temperatura do chassi do controlador de computação	O status da temperatura do controlador de computação.

+

Coluna na tabela prateleiras de armazenamento	Descrição
Número de série do chassi do compartimento	O número de série do chassi do compartimento de armazenamento.

Coluna na tabela prateleiras de armazenamento	Descrição
ID do compartimento	O identificador numérico da prateleira de armazenamento. • 99: Compartimento do controlador de storage • 0: Primeira prateleira de expansão • 1: Segunda prateleira de expansão **Nota:** as prateleiras de expansão aplicam-se apenas aos modelos SG6060 e SG6160.
Status do compartimento	O status geral da gaveta de storage.
Estado IOM	O status dos módulos de entrada/saída (IOMs) em quaisquer prateleiras de expansão. N/A se este não for um compartimento de expansão.
Estado da fonte de alimentação	O status geral das fontes de alimentação para o compartimento de armazenamento.
Estado da gaveta	O estado das gavetas na prateleira de arrumação. N/A se a prateleira não contiver gavetas.
Estado da ventoinha	O status geral dos ventiladores de resfriamento na prateleira de armazenamento.
Slots de unidade	O número total de slots de unidade no compartimento de armazenamento.
Unidades de dados	O número de unidades no compartimento de storage usadas para o storage de dados.
tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados no compartimento de storage.
Unidades de cache	O número de unidades no compartimento de armazenamento que são usadas como cache.
Tamanho da unidade de cache	O tamanho da menor unidade de cache no compartimento de armazenamento. Normalmente, as unidades de cache têm o mesmo tamanho.
Estado da configuração	O status de configuração do compartimento de storage.

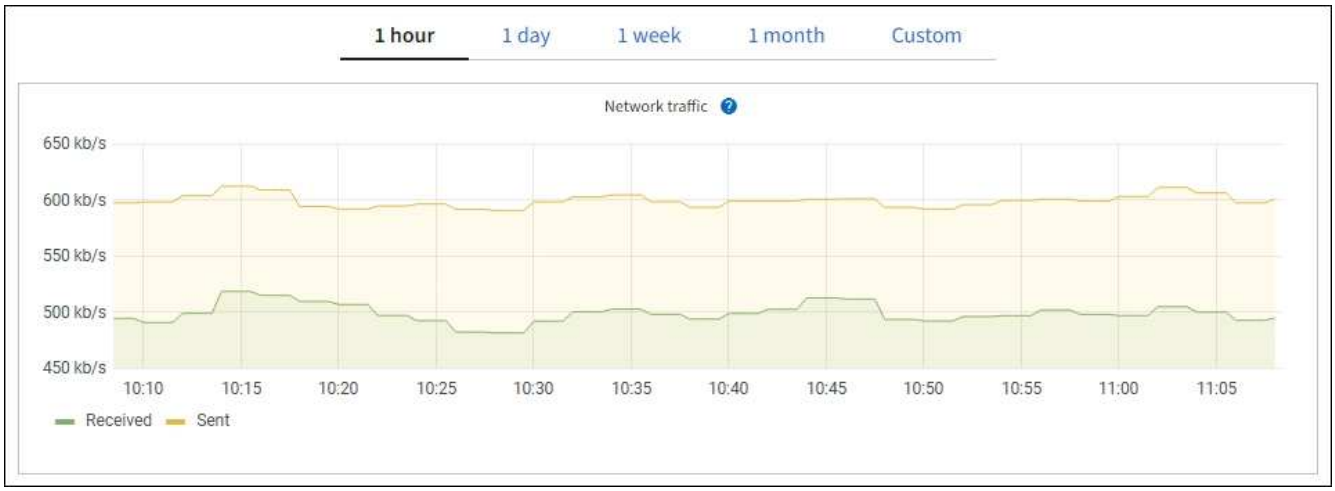
a. Confirmar se todos os Estados são "nominais".

   Se um estado não for "nominal", reveja quaisquer alertas atuais. Você também pode usar o

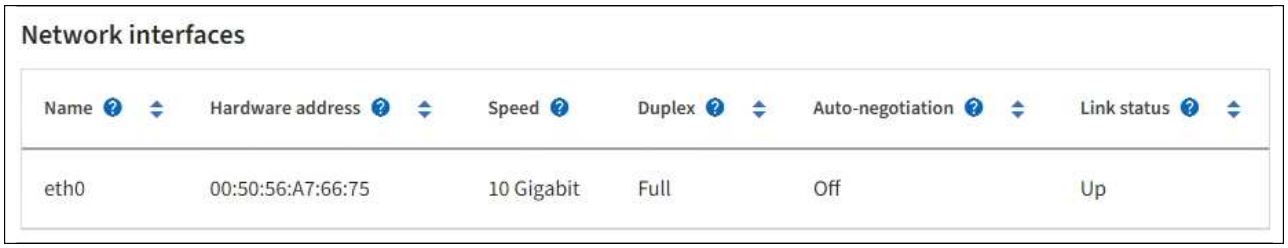
Gerenciador de sistema do SANtricity para saber mais sobre alguns desses valores de hardware. Consulte as instruções para instalar e manter o seu aparelho.

4. Selecione **rede** para ver as informações de cada rede.

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



   a. Reveja a secção interfaces de rede.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

   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/backup ou o modo LACP.

   Os valores mostrados na tabela assumem que todos os quatro links são usados.

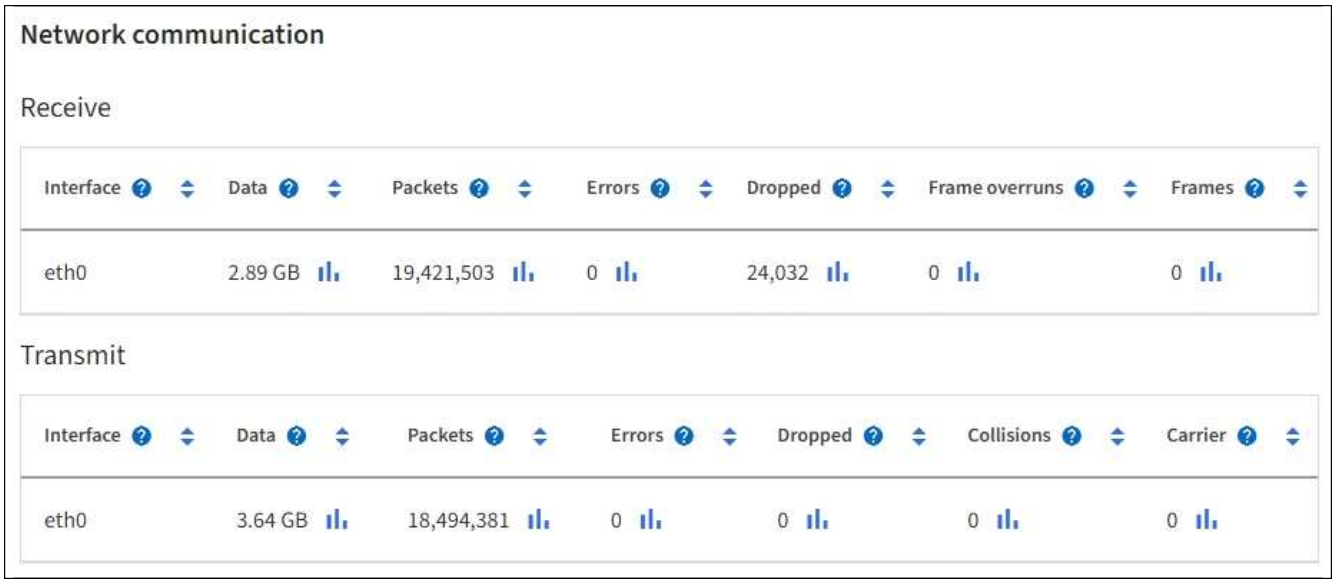
Modo de ligação	Modo Bond	Velocidade de ligação HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede do cliente/grade (eth0,eth2)
Agregado	LACP	25	100
Fixo	LACP	25	50
Fixo	Ativo/Backup	25	25
Agregado	LACP	10	40
Fixo	LACP	10	20

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

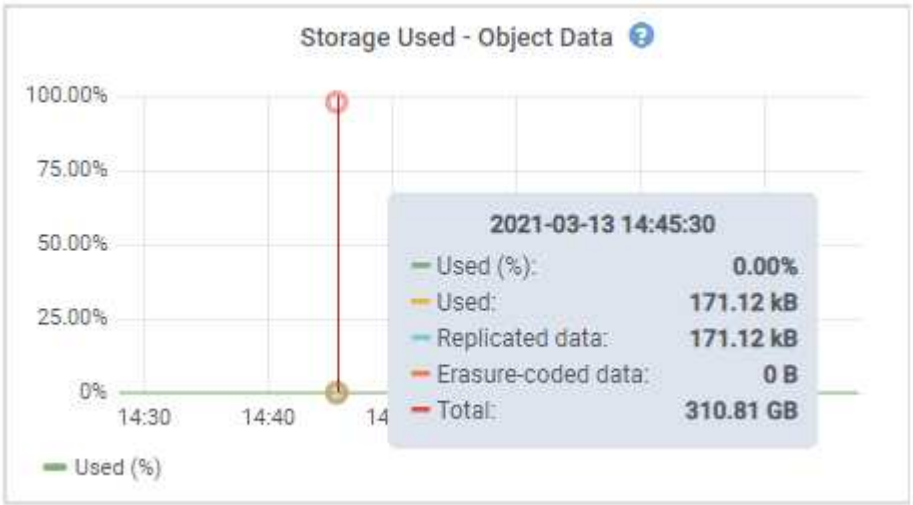
Consulte "Configurar ligações de rede" para obter mais informações sobre como configurar as portas 10/25-GbE.

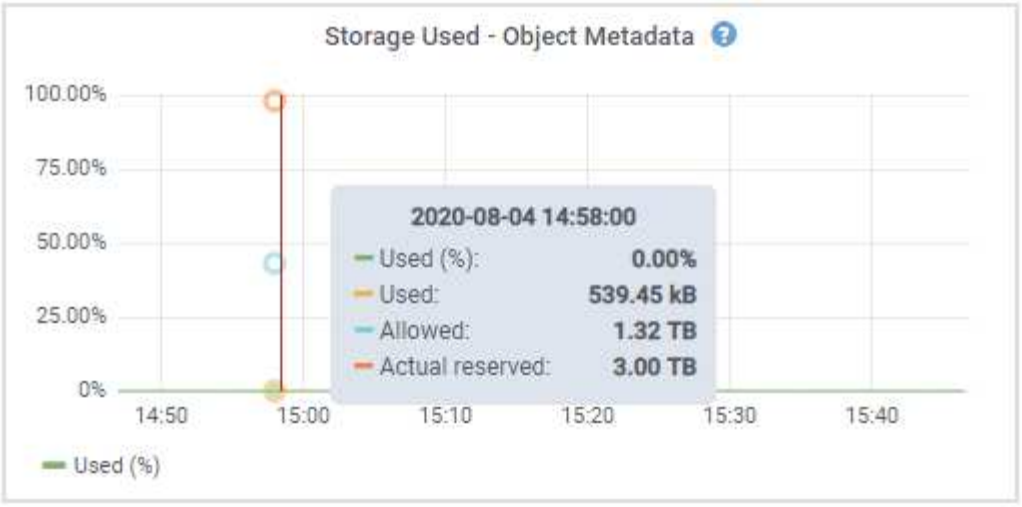
b. Reveja a secção Comunicação de rede.

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

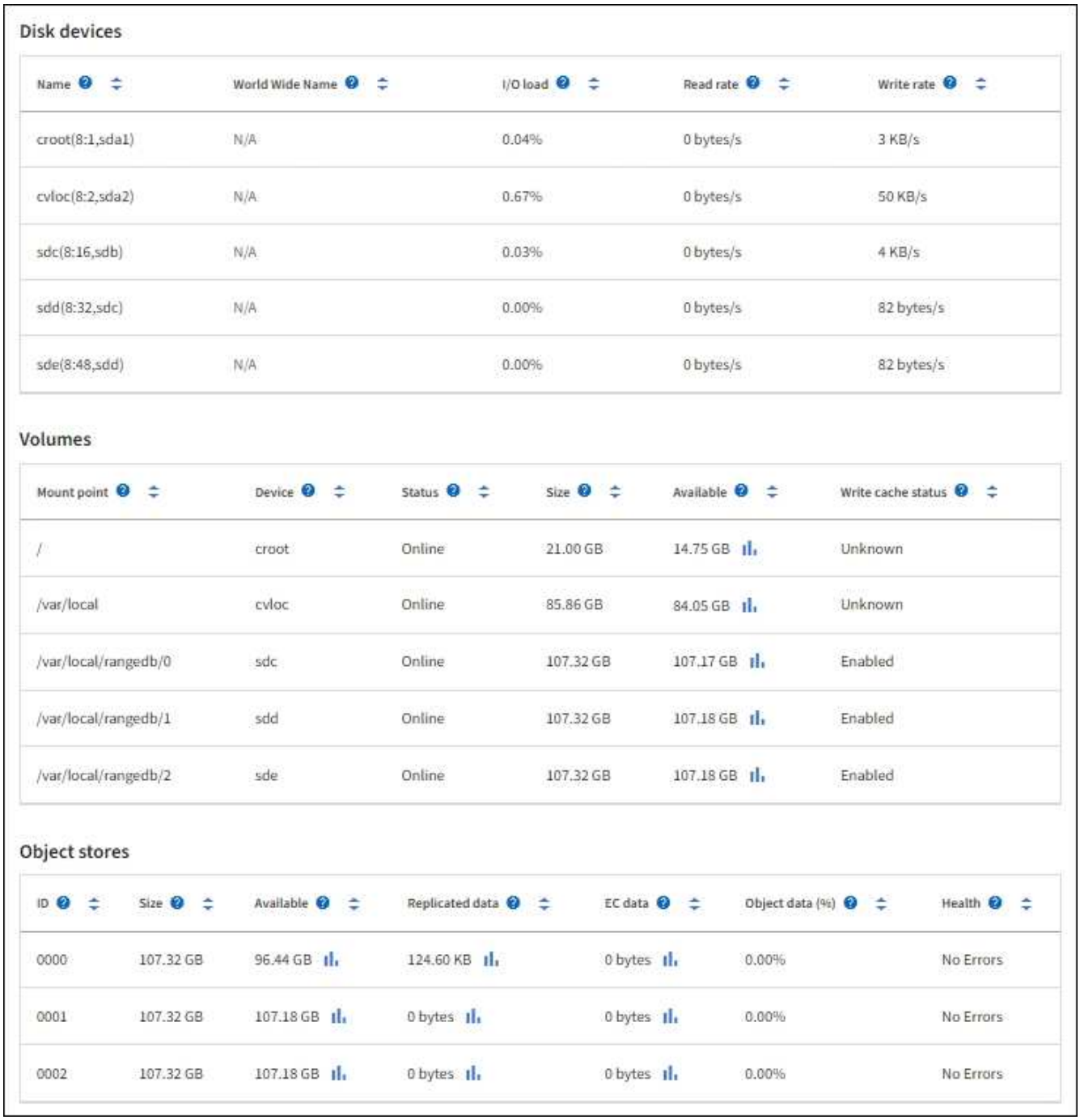




a. Role para baixo para ver as quantidades de armazenamento disponível para cada volume e armazenamento de objetos.

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

   Para ajudá-lo a interpretar estatísticas de leitura e gravação de disco relacionadas aos pontos de montagem de volume, a primeira parte do nome mostrado na coluna **Nome** da tabela dispositivos de disco (ou seja, *sdc*, *sdd*, *sde*, etc.) 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 os nós de administração do dispositivo e os nós de gateway

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 serviços que é usado como nó de administrador ou 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.

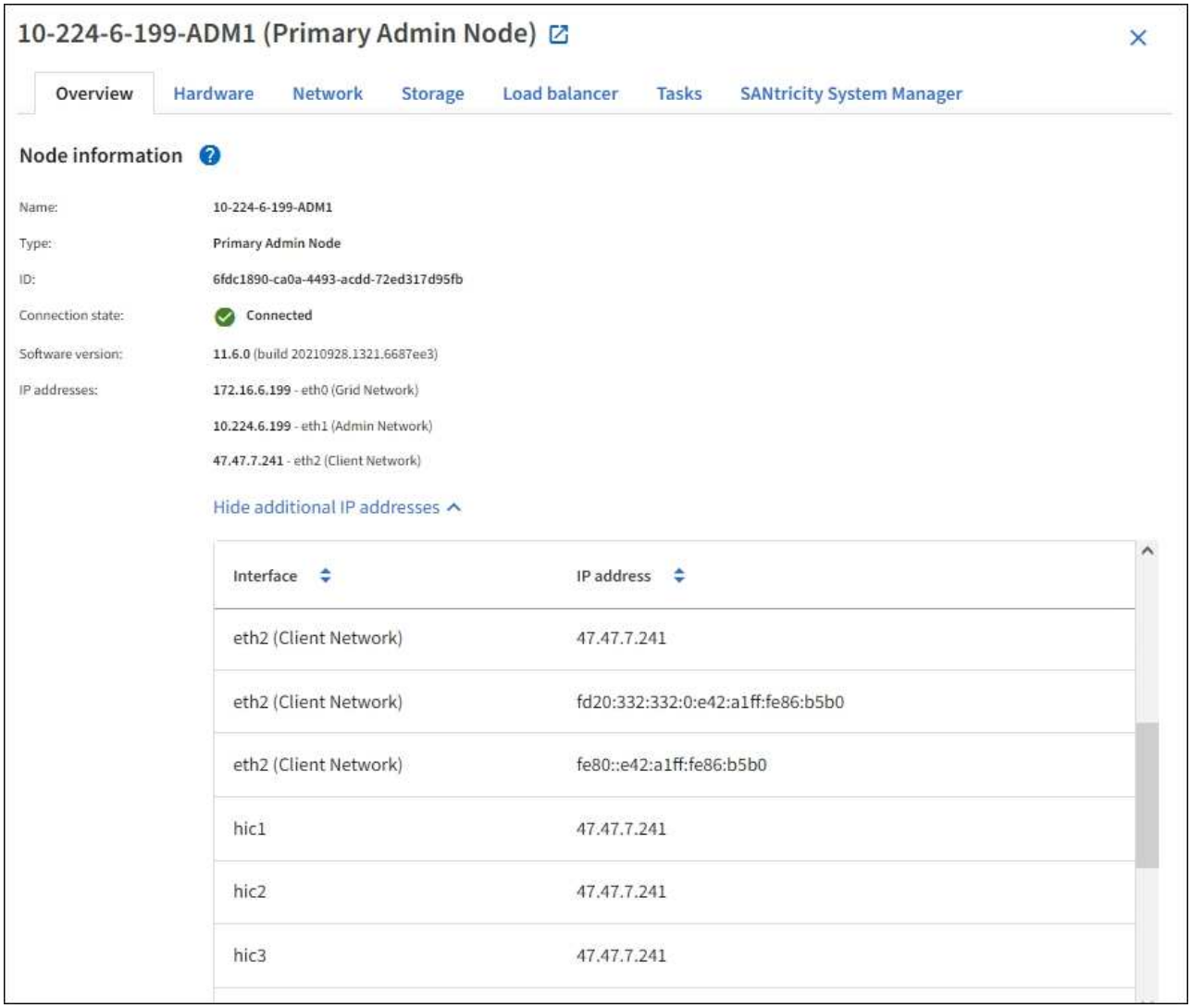
Passos

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 do nó. A lista de endereços IP inclui o nome da interface para cada endereço, da

seguinte forma:

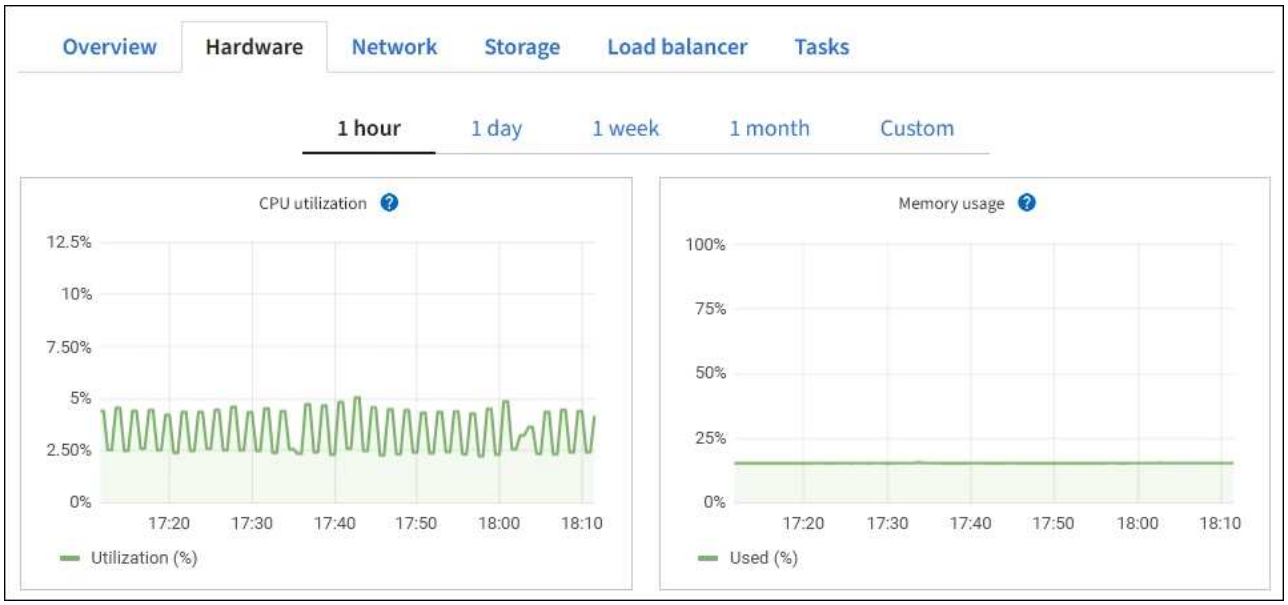
- **Adllb** e **adlli**: Mostrado se a ligação ativa/backup é usada para a interface Admin Network
- **eth**: Rede de Grade, rede Admin ou rede de cliente.
- **Hic**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Estas portas podem ser Unidas e ligadas à rede de grelha StorageGRID (eth0) e à rede de clientes (eth2).
- **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são ligadas para formar a interface de rede Admin (eth1). Pode deixar outras interfaces mtc disponíveis para conetividade local temporária para um técnico no centro de dados.



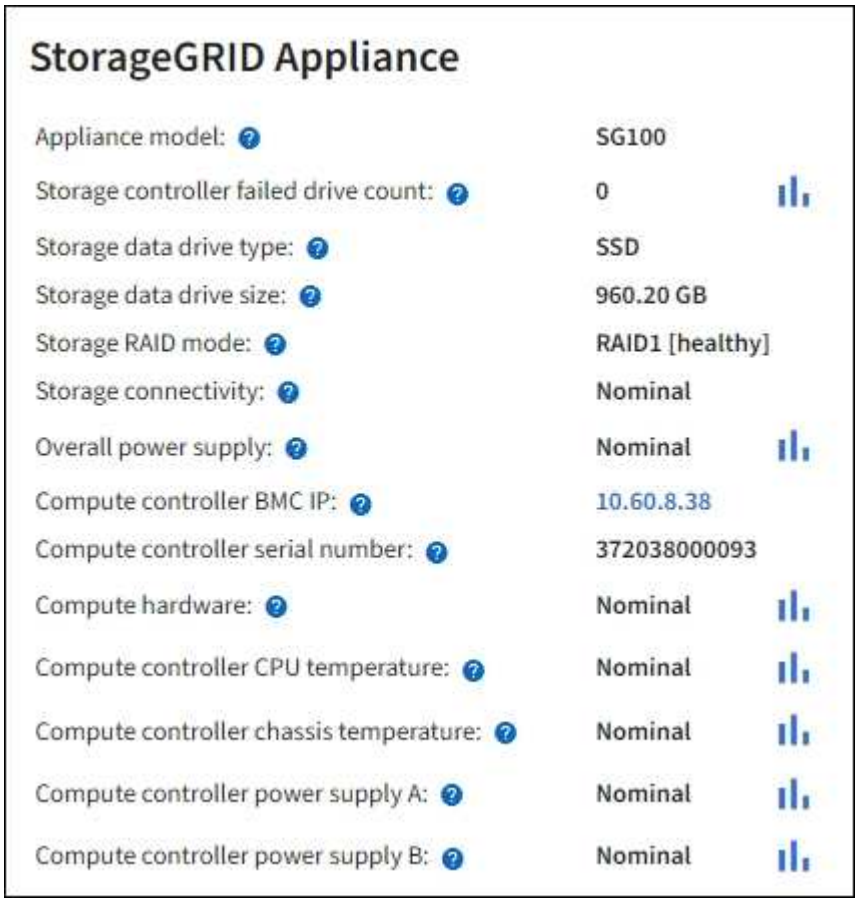
A seção Alertas da guia Visão geral exibe quaisquer alertas ativos para o nó.

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

   a. Visualize os gráficos de utilização da CPU e memória para determinar as percentagens de utilização da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico ou 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, o número de série, a versão do firmware do controlador e o status de cada componente.



Campo na mesa do aparelho	Descrição
Modelo do aparelho	O número do modelo para este dispositivo StorageGRID.

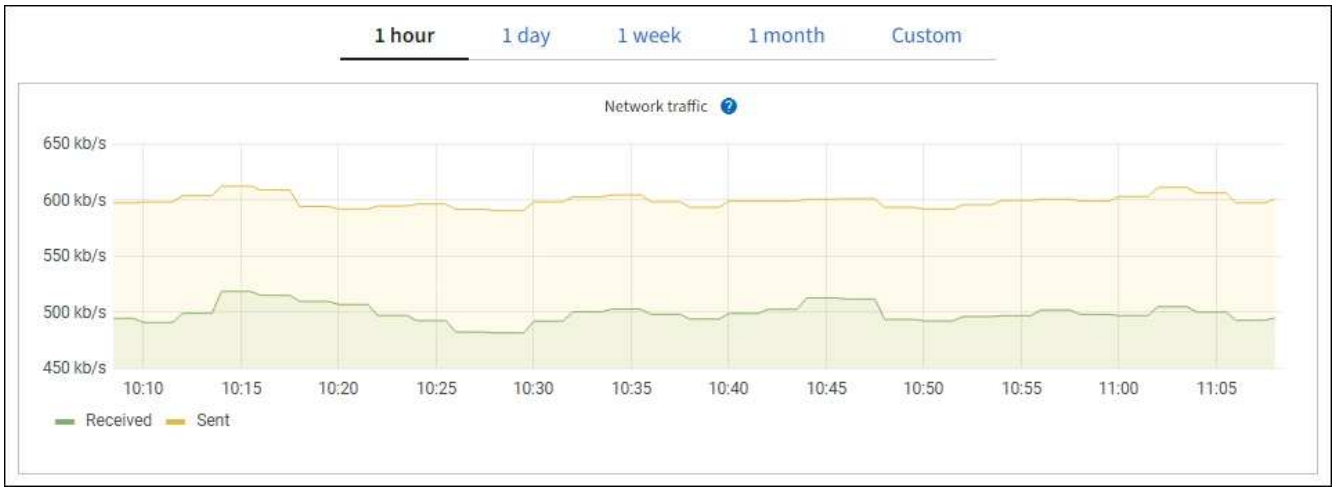
Campo na mesa do aparelho	Descrição
Falha na contagem de unidades do controlador de armazenamento	O número de unidades que não são ideais.
Tipo de unidade de dados de armazenamento	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de dados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

a. Confirmar se todos os Estados são "nominais".

   Se um estado não for "nominal", reveja quaisquer alertas atuais.

4. Selecione **rede** para ver as informações de cada rede.

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



a. Reveja a secção 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

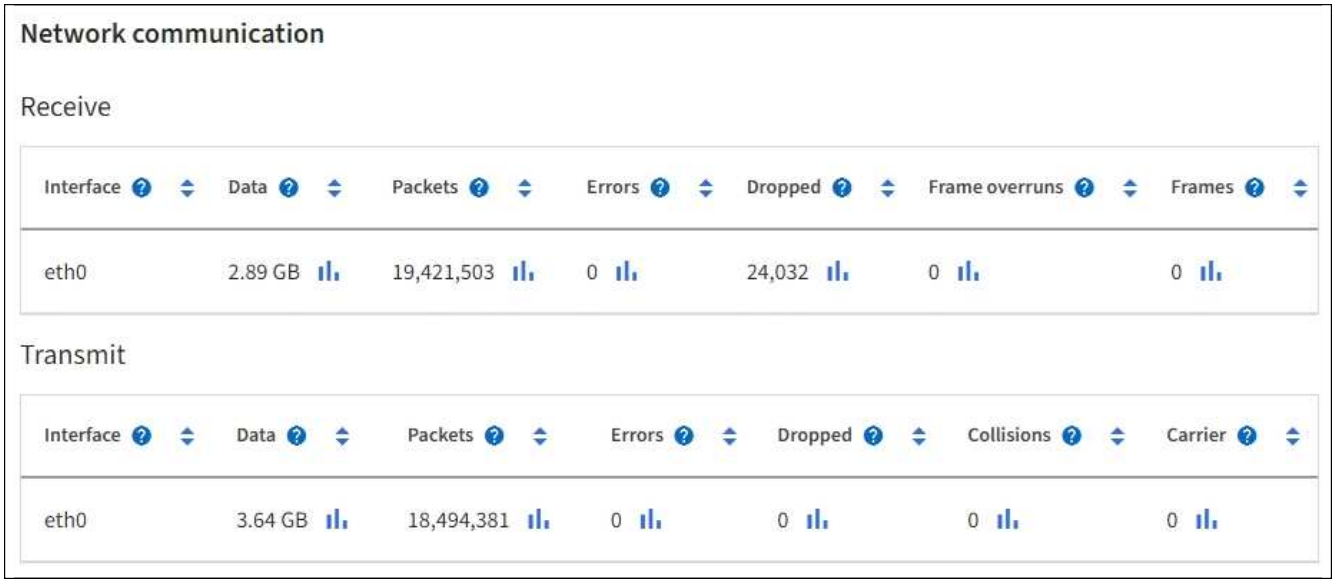
Use a tabela a seguir com os valores na coluna **velocidade** na tabela interfaces de rede para determinar se as quatro portas de rede 40/100-GbE no dispositivo foram configuradas para usar o modo ativo/backup ou o modo LACP.

Os valores mostrados na tabela assumem que todos os quatro links são usados.

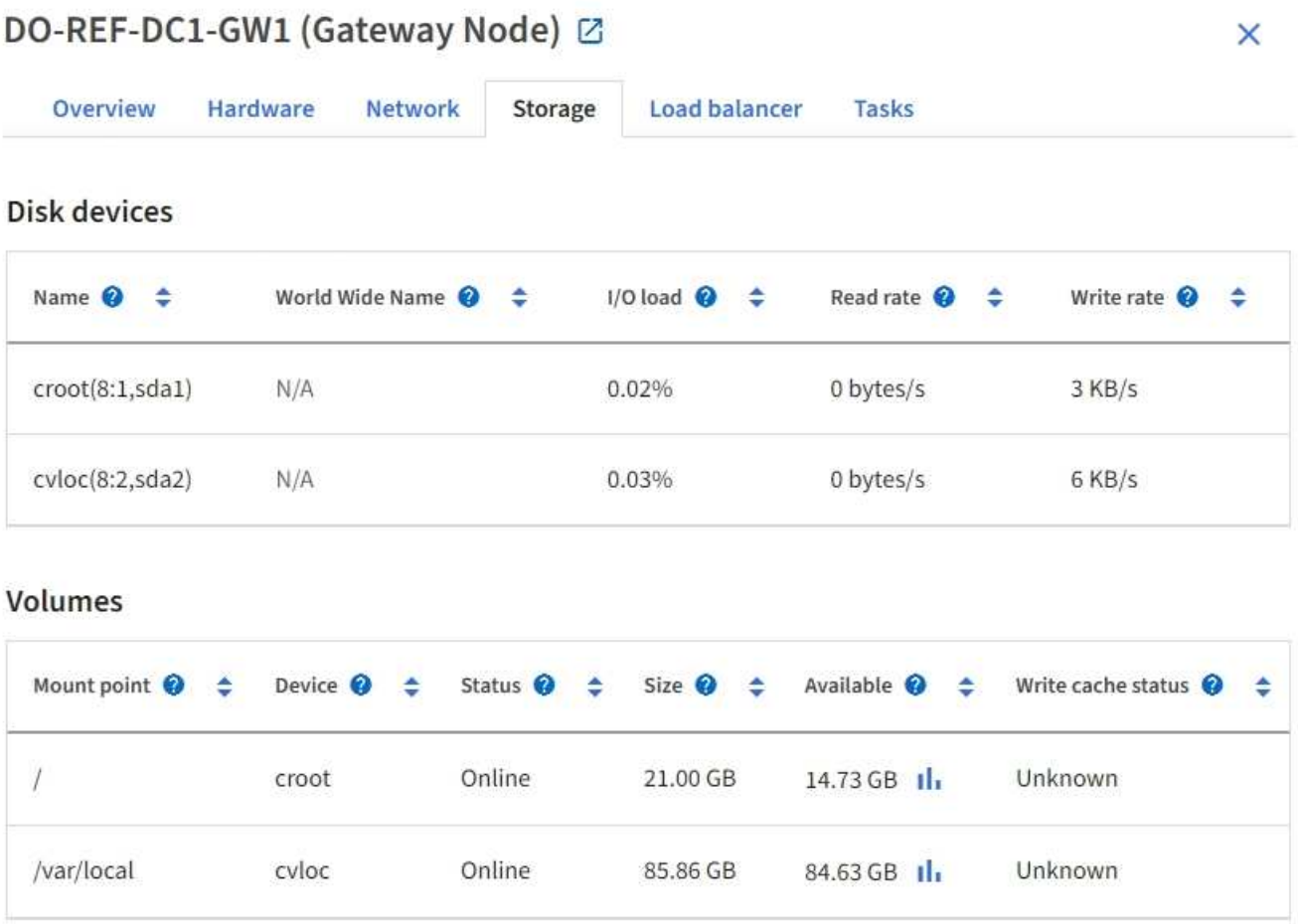
Modo de ligação	Modo Bond	Velocidade de ligação HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede do cliente/grade (eth0, eth2)
Agregado	LACP	100	400
Fixo	LACP	100	200
Fixo	Ativo/Backup	100	100
Agregado	LACP	40	160
Fixo	LACP	40	80
Fixo	Ativo/Backup	40	40

b. Reveja a secção Comunicação de rede.

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



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



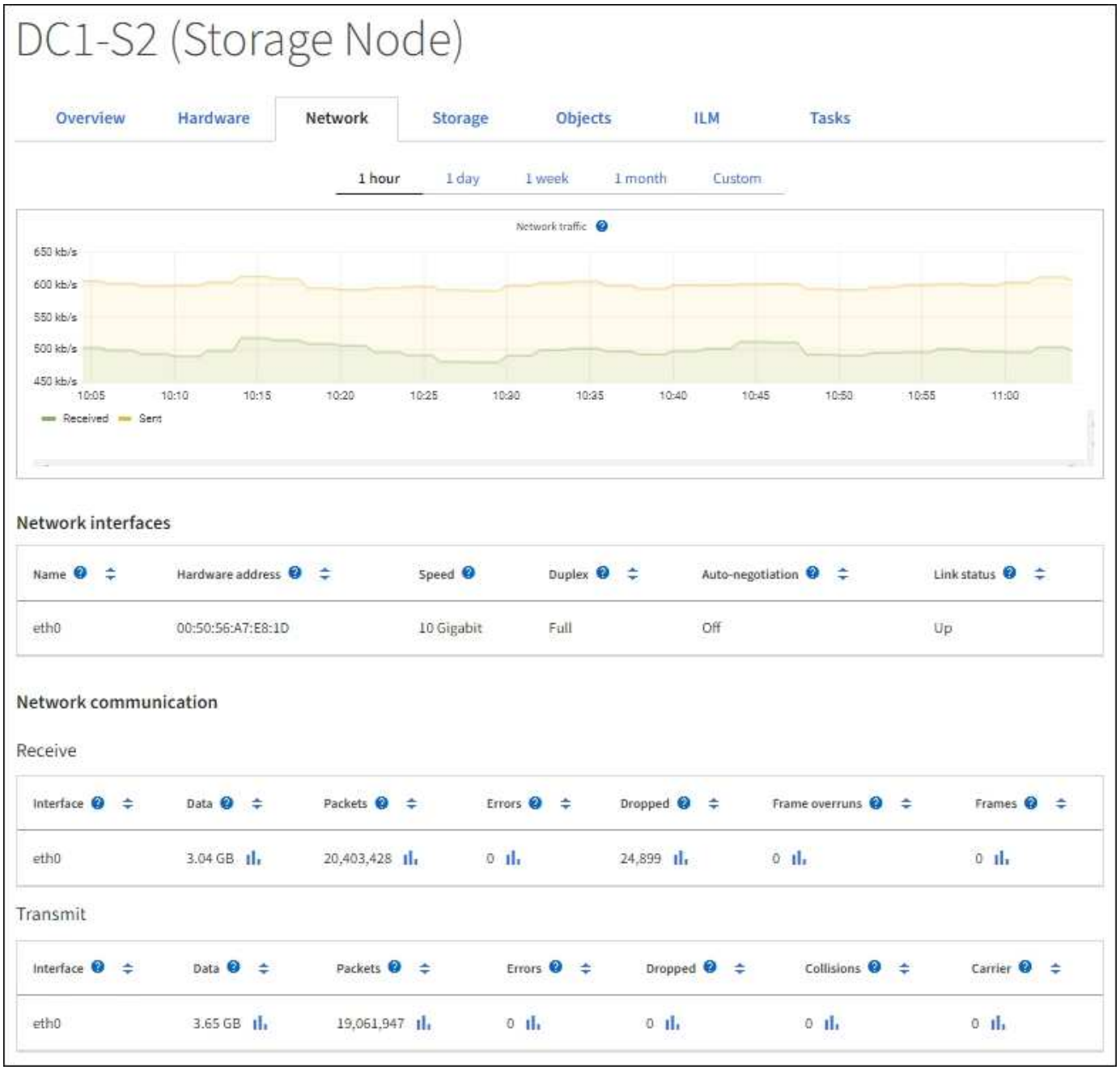
Veja a guia rede

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 ou 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 receção e transmissão de cada nó e quaisquer contadores de falhas comunicados pelo condutor.



Informações relacionadas

"Monitorar conexões de rede e desempenho"

Exibir a guia armazenamento

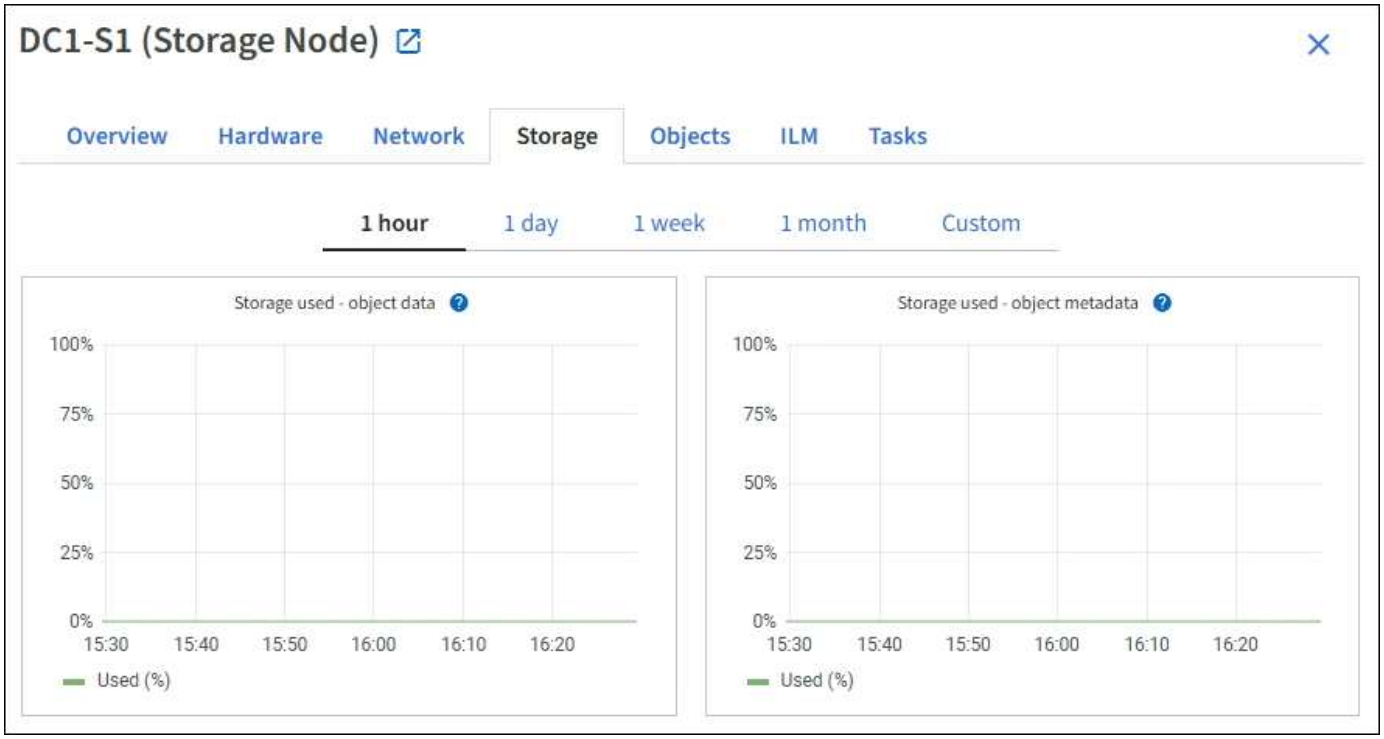
A guia armazenamento resume a disponibilidade de armazenamento e outras métricas de armazenamento.

A guia Storage (armazenamento) é exibida para todos os nós, cada local e toda a grade.

Armazenamento de gráficos usados

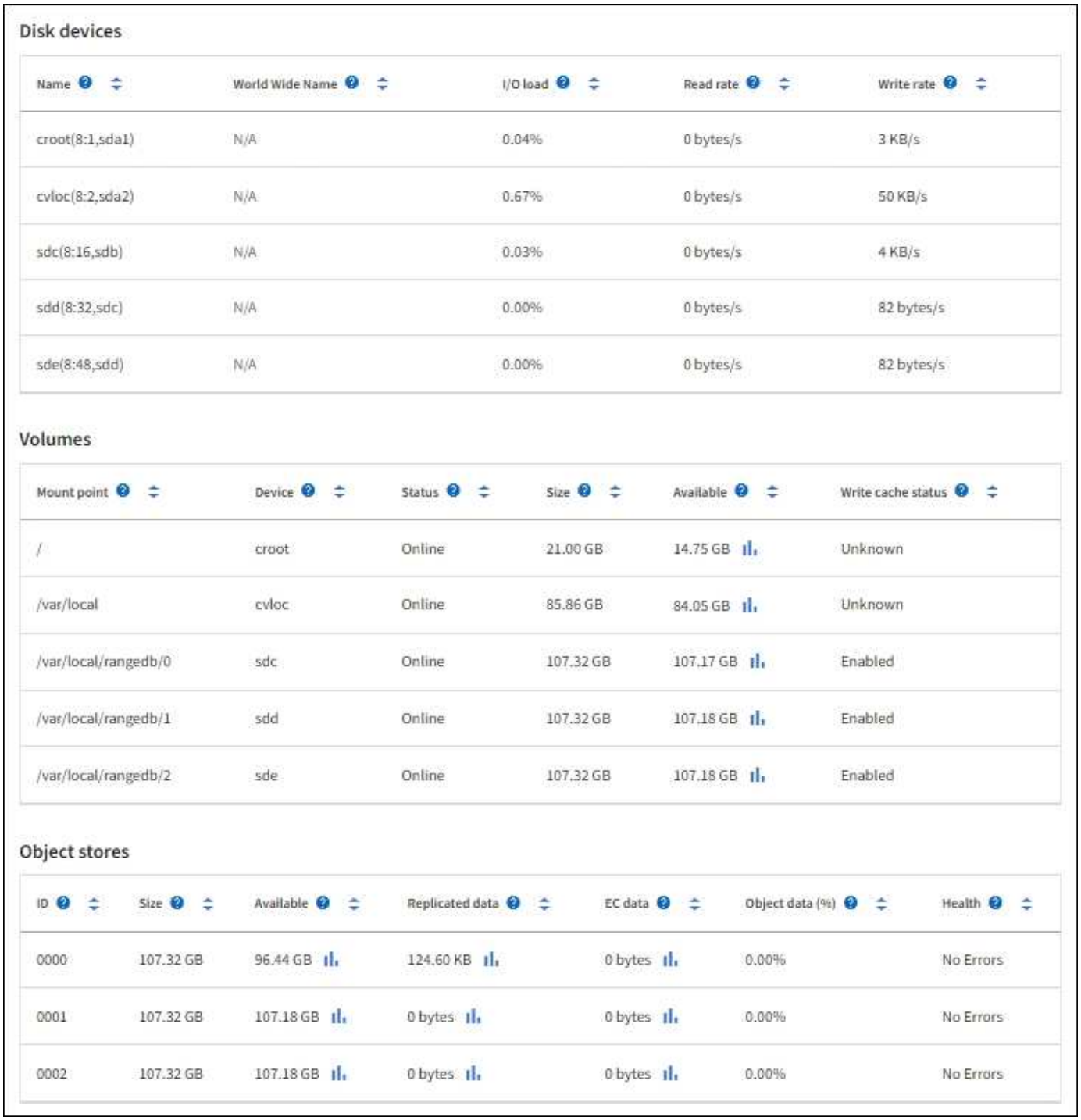
Para nós de storage, cada local e toda a grade, a guia Storage inclui gráficos mostrando quanto de storage foi usado pelos dados de objeto e metadados de objeto ao longo do tempo.

Quando um nó não está conetado à grade, como durante a atualização ou um estado desconetado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da grade. Depois que um nó se reconeta à grade, espere vários minutos para que os valores se estabilizem.



Dispositivos de disco, volumes e objetos armazenam tabelas

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



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

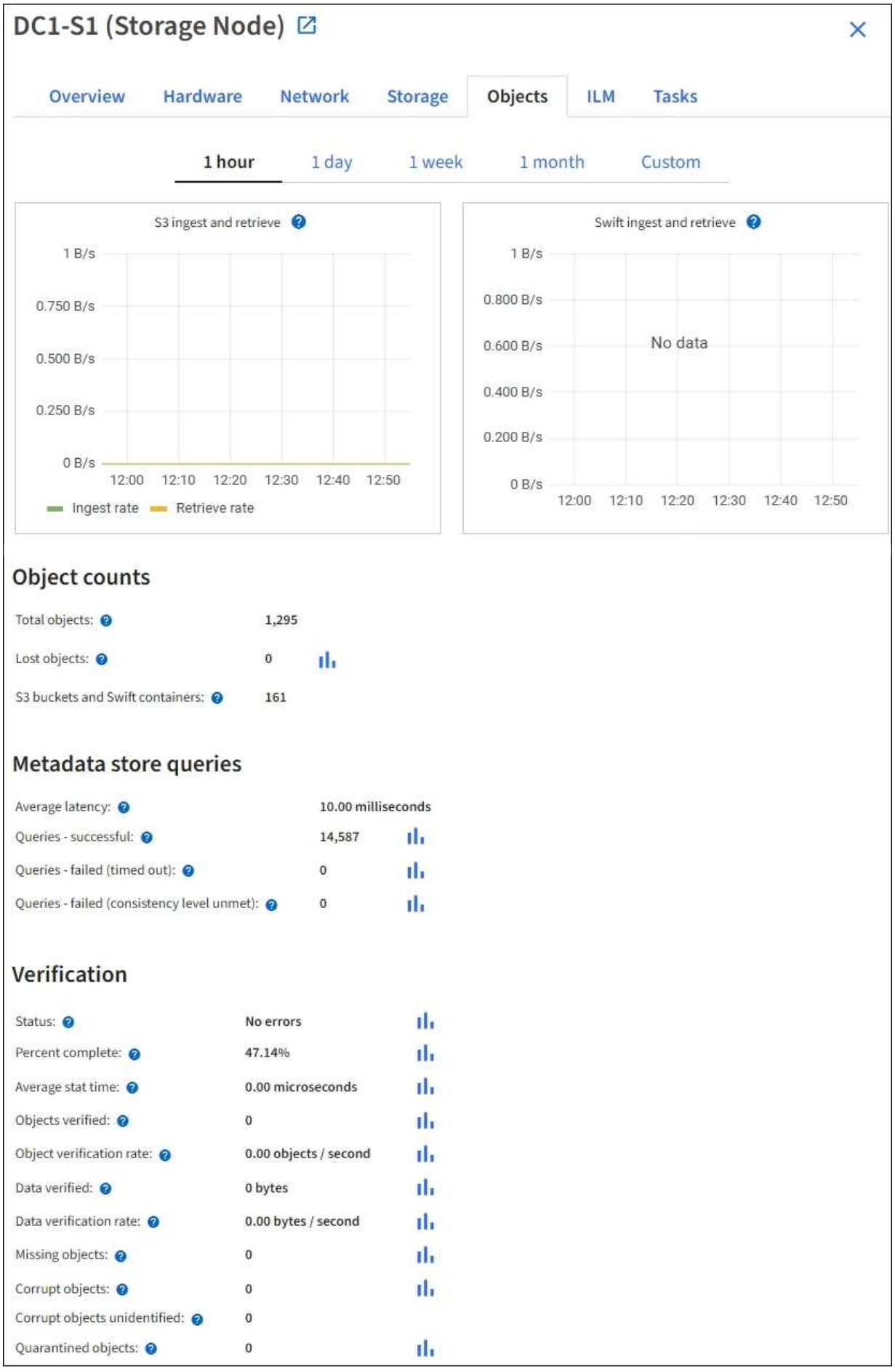
Informações relacionadas

"Monitorar a capacidade de armazenamento"

Exibir a guia objetos

A guia objetos fornece informações sobre "S3"taxas de ingestão e "Rápido"recuperação.

A guia objetos é exibida para cada nó de armazenamento, cada local e toda a grade. Para nós de storage, a guia objetos também fornece contagens de objetos e informações sobre consultas de metadados e verificação em segundo plano.

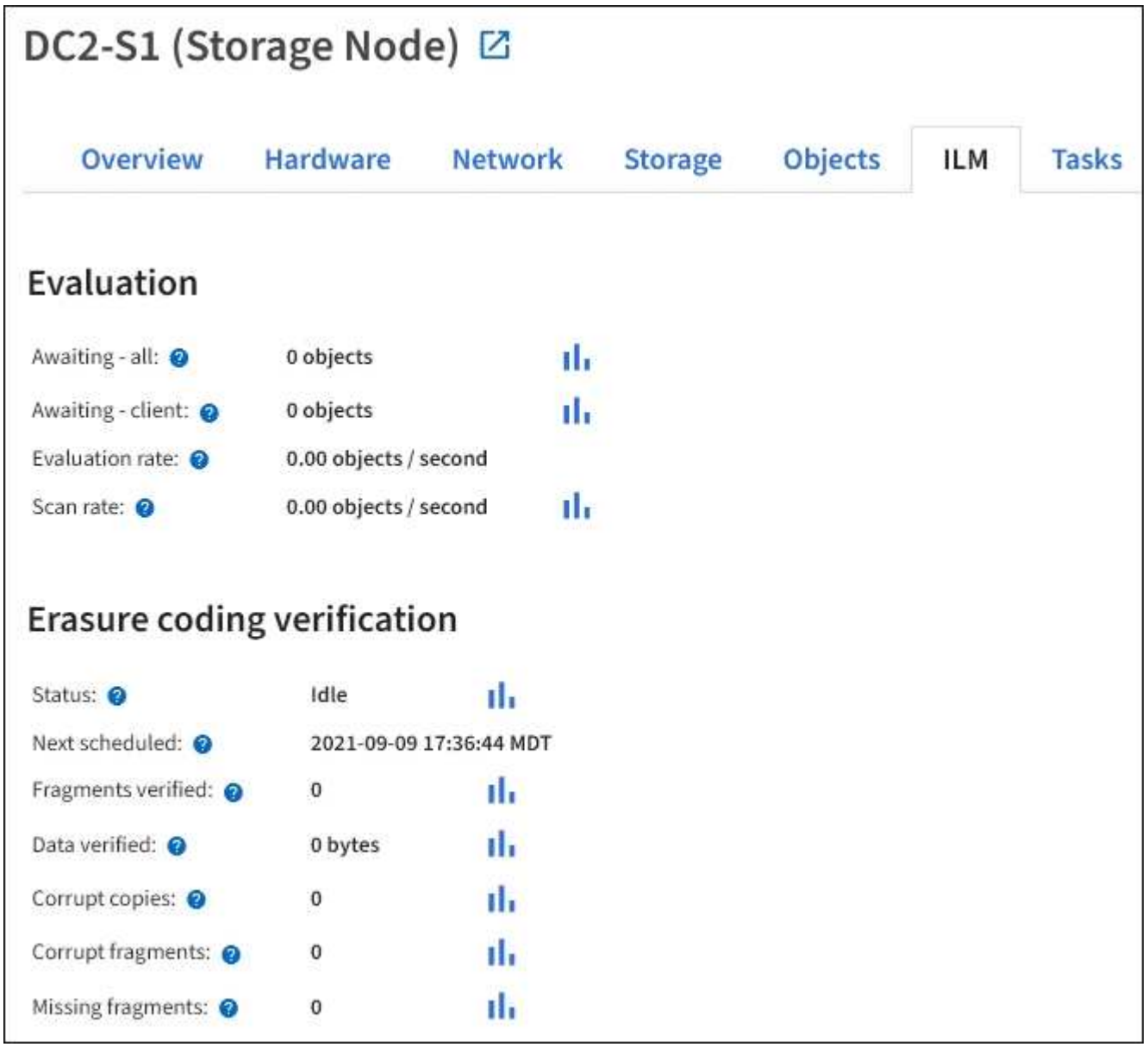

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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

Veja a guia ILM

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

A guia ILM é mostrada para cada nó de armazenamento, cada local e toda a grade. Para cada local e grade, a guia ILM mostra um gráfico da fila 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 storage, a guia ILM fornece detalhes sobre a avaliação ILM e a verificação em segundo plano para objetos codificados por apagamento.



Informações relacionadas

"Monitorar o gerenciamento do ciclo de vida das informações"

"Administrar o StorageGRID"

Use a guia tarefas

A guia tarefas é exibida para todos os nós. Você pode usar essa guia para renomear ou reinicializar um nó ou colocar um nó de appliance no modo de manutenção.

Para obter os requisitos e instruções completos para cada opção neste separador, consulte o seguinte:

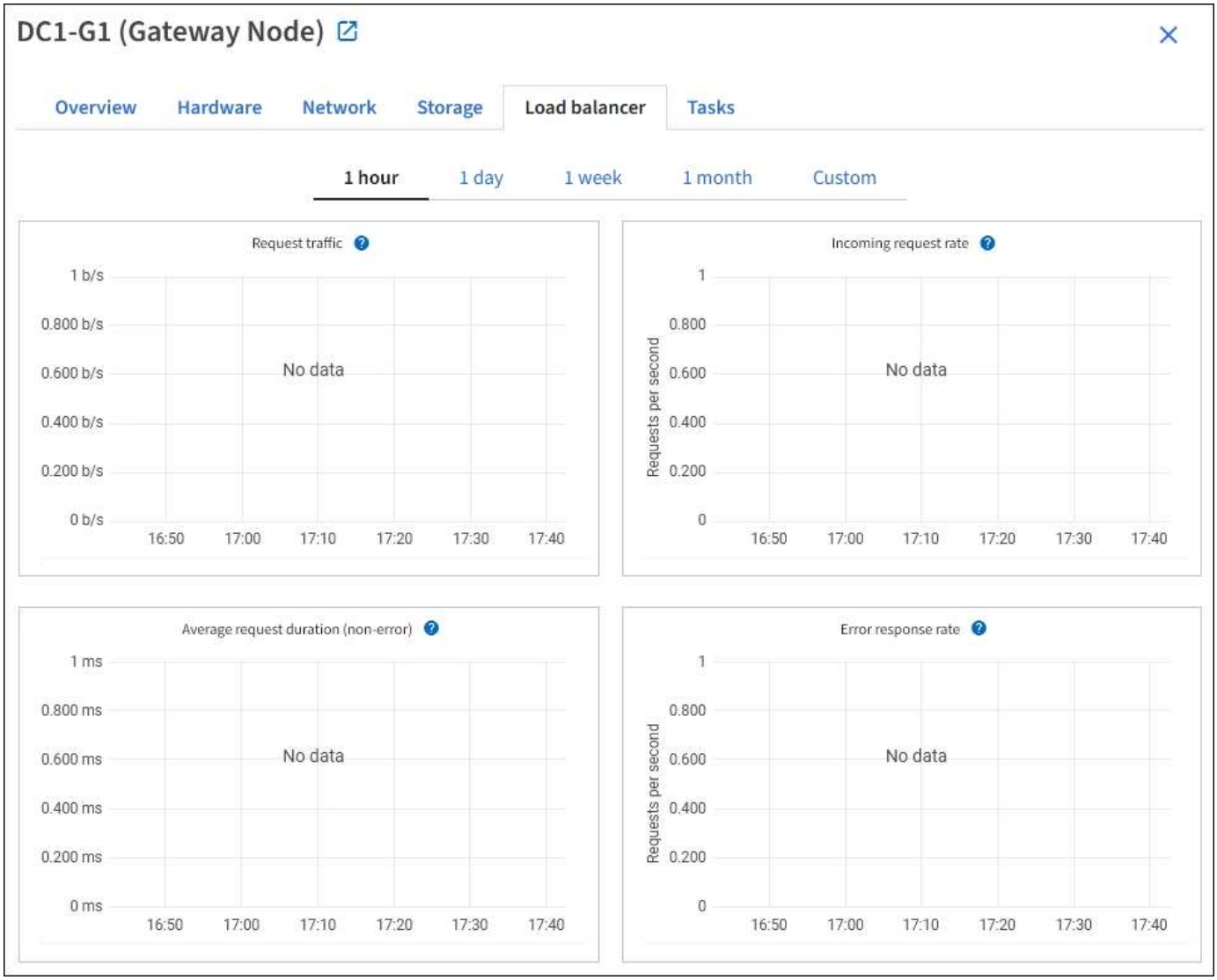
- "Renomeie grade, sites e nós"
- "Reinicie o nó da grade"
- "Coloque o aparelho no modo de manutenção"

Veja a guia balanceador de carga

O separador Load Balancer (balanceador de carga) inclui gráficos de desempenho e diagnóstico relacionados com o funcionamento do serviço Load Balancer.

A guia Load Balancer (balanceador de carga) é exibida para nós de administração e nós de gateway, cada local e toda a grade. Para cada local, a guia Load Balancer fornece um resumo agregado das estatísticas de todos os nós nesse local. Para toda a grade, a guia Load Balancer fornece um resumo agregado das estatísticas de todos os sites.

Se não houver nenhuma e/S sendo executada pelo serviço do Load Balancer ou se não houver nenhum balanceador de carga configurado, os gráficos exibem "no data".



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.

> Esse valor é atualizado na conclusão de cada solicitação. Como resultado, esse valor pode diferir do throughput em tempo real a taxas de solicitação baixas ou para solicitações de muito tempo. Você pode olhar para a guia rede para obter uma visão mais realista do comportamento atual da rede.

Taxa de solicitação recebida

Este gráfico fornece uma média móvel de 3 minutos do número de novas solicitações por segundo, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Este valor é atualizado quando os cabeçalhos de uma nova solicitação tiverem sido validados.

Duração média da solicitação (sem erro)

Este gráfico fornece uma média móvel de 3 minutos de duração de solicitações, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Cada duração da 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, discriminada pelo código de resposta de erro.

Informações relacionadas

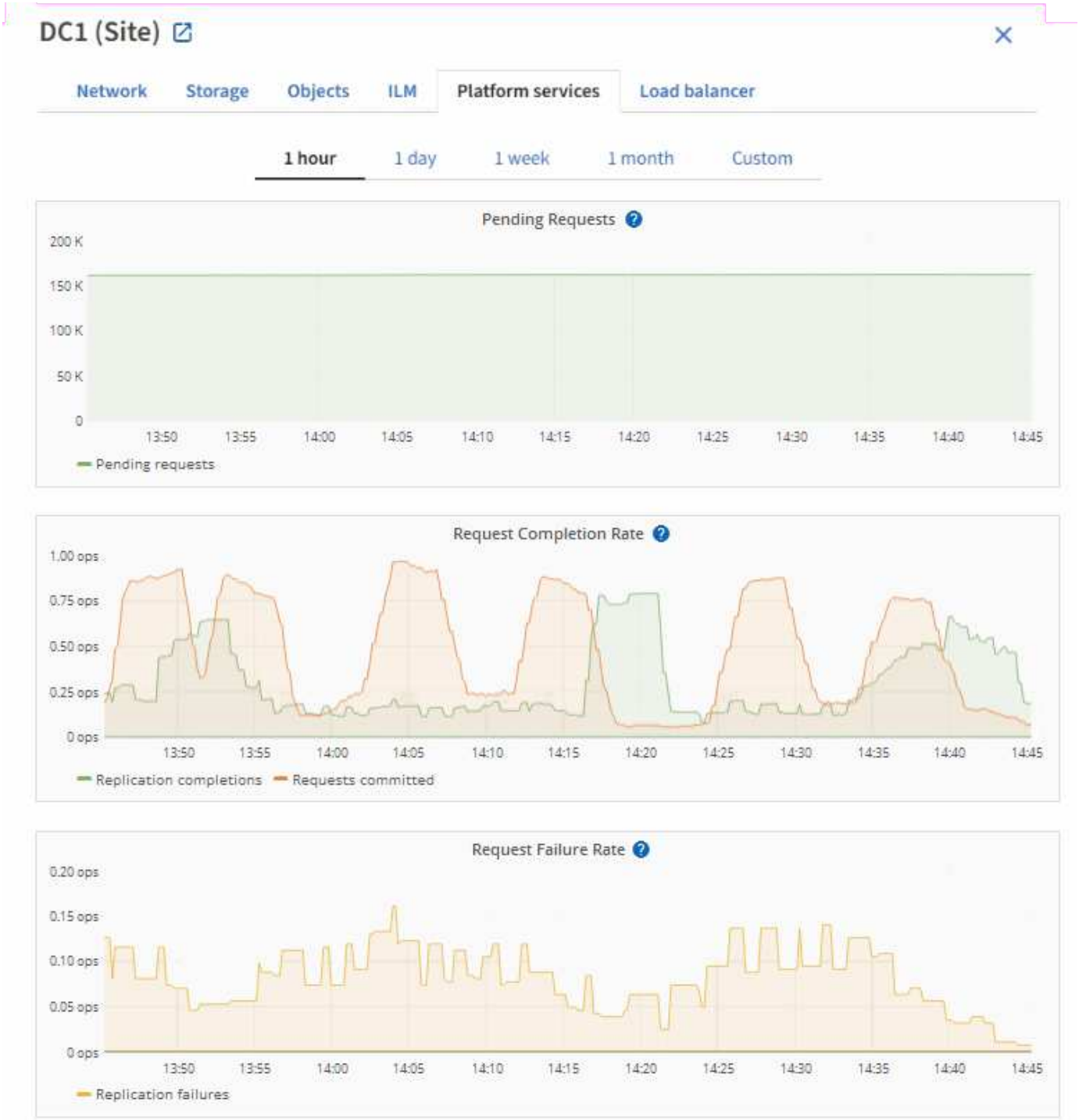
"Monitorar operações de balanceamento de carga"

"Administrar o StorageGRID"

Veja a guia Serviços da Plataforma

A guia Serviços da plataforma fornece informações sobre qualquer operação de serviço da plataforma S3 em um site.

A guia Serviços da Plataforma é exibida para cada site. Esta guia fornece informações sobre os serviços da plataforma S3, como 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 (somente SGF6112)

A guia Gerenciar unidades permite acessar detalhes e executar tarefas de solução de problemas e manutenção nas unidades no dispositivo SGF6112.

A guia Gerenciar unidades é exibida somente para nós de dispositivos de storage do SGF6112.

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

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

Para acessar a guia Gerenciar unidades, você deve ter o "Administrador do dispositivo de storage ou permissão de acesso à raiz".

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

Exibir a guia Gerenciador de sistema do SANtricity (somente Série e)

A guia Gerenciador de sistema do SANtricity permite que você acesse o Gerenciador de sistema do SANtricity sem ter que configurar ou conetar a porta de gerenciamento do dispositivo de storage. Pode utilizar este separador para rever as informações ambientais e de diagnóstico de hardware, bem como os problemas relacionados com as unidades.

A guia Gerenciador de sistema do SANtricity é exibida somente para nós de dispositivos de storage que usam o hardware e-Series.

Usando o Gerenciador de sistema do SANtricity, você pode fazer o seguinte:

- Visualize dados de performance, como performance em nível de array de storage, latência de e/S, utilização de CPU com controladora de storage e taxa de transferência.
- Verifique o status do componente do hardware.
- Execute funções de suporte, incluindo visualização de dados de diagnóstico e configuração do e-Series AutoSupport.

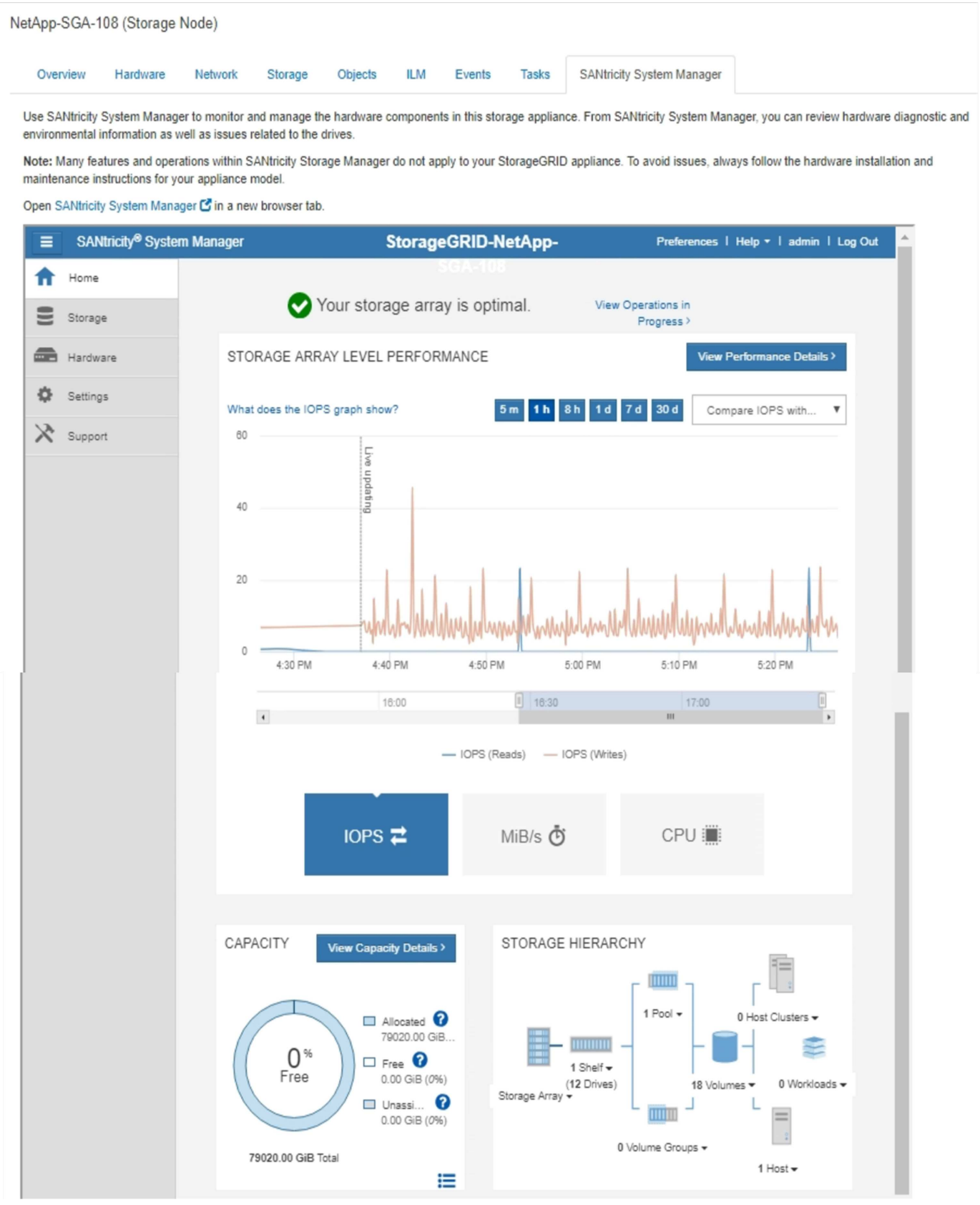
Para usar o Gerenciador de sistema do SANtricity para configurar um proxy para o e-Series AutoSupport, "Envie pacotes e-Series AutoSupport através do StorageGRID"consulte .

Para acessar o Gerenciador de sistema do SANtricity por meio do Gerenciador de Grade, você deve ter o "Administrador do dispositivo de storage ou permissão de acesso à raiz".

Você deve ter o firmware SANtricity 8,70 ou superior para acessar o Gerenciador de sistema do SANtricity usando o Gerenciador de Grade.

O acesso ao Gerenciador de sistemas do SANtricity a partir do Gerenciador de Grade geralmente se destina apenas a monitorar o hardware do dispositivo e configurar o e-Series AutoSupport. Muitos recursos e operações dentro do Gerenciador de sistema do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de manutenção de hardware do seu aparelho.

O separador apresenta a página inicial do Gestor do sistema SANtricity.



Você pode usar o link Gerenciador de sistema do SANtricity para abrir o Gerenciador de sistema do SANtricity em uma nova janela do navegador para facilitar a visualização.

Para ver detalhes sobre o desempenho do nível de storage e o uso da capacidade, posicione o cursor sobre

cada gráfico.

Para obter mais detalhes sobre como exibir as informações acessíveis na guia Gerenciador do sistema do SANtricity, "Documentação do NetApp e-Series e do SANtricity" consulte .

Informações para monitorar regularmente

O que e quando monitorar

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

Antes de começar

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

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 de forma contínua.

O que monitorar	Frequência
"Estado de integridade do sistema"	Diariamente
Taxa em que "Capacidade de metadados e objetos do nó de storage"está sendo consumido	Semanalmente
"Operações de gerenciamento do ciclo de vida das informações"	Semanalmente
"Recursos de rede e sistema"	Semanalmente
"Atividade do locatário"	Semanalmente
"Operações de clientes S3 e Swift"	Semanalmente
"Operações de balanceamento de carga"	Após a configuração inicial e após quaisquer alterações de configuração
"Conexões de federação de grade"	Semanalmente
"Capacidade do sistema de armazenamento de arquivos externo"	Semanalmente

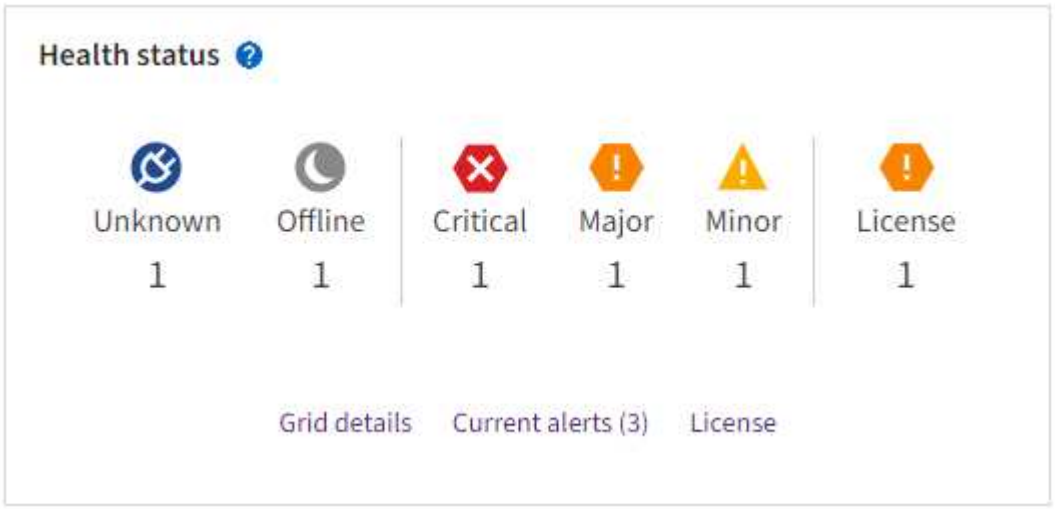
Monitorar a integridade do sistema

Monitore diariamente a integridade geral do seu sistema StorageGRID.

Sobre esta tarefa

O sistema StorageGRID pode continuar a funcionar quando partes da grelha não estiverem disponíveis. Problemas potenciais indicados por alertas ou alarmes (sistema legado) não são necessariamente problemas com as operações do sistema. Investigue problemas resumidos na placa de estado de funcionamento do Painel do Grid Manager.

Para ser notificado de alertas assim que eles são acionados, você pode "configurar notificações por e-mail para alertas" ou "Configurar traps SNMP".



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

Link	Aparece quando…
Detalhes da grelha	Todos os nós são desconetados (estado de conexão desconhecido ou administrativamente inativo).
Alertas atuais (crítico, maior, menor)	Os alertas são atualmente ativo.
Alertas resolvidos recentemente	Alertas disparados na semana estão agora resolvidospassada .
Licença	Existe um problema com a licença de software para este sistema StorageGRID. Você pode "atualize as informações da licença conforme necessário".

Monitorar os estados de conexão do nó

Se um ou mais nós forem desconetados da grade, as operações críticas do StorageGRID podem ser afetadas. Monitore os estados de conexão dos nós e solucione quaisquer problemas imediatamente.

Ícone	Descrição	Ação necessária
	Não ligado - desconhecido Por um motivo desconhecido, um nó é desconetado ou os serviços no nó estão inalterados inesperadamente. 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 é possível se 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 tenha parado ou reiniciado o host para o nó. **Nota**: Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.
	Não conetado - administrativamente para baixo Por um motivo esperado, o nó não está conetado à grade. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam online sem nenhuma intervenção.	Determine se algum alerta está afetando esse nó. Se um ou mais alertas estiverem ativos selecione cada alertae siga as ações recomendadas.
	Conectado O nó está conetado à grade.	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 "as notificações por e-mail de alerta estão 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 para o StorageGRID 11,8"

A tabela a seguir descreve as informações mostradas no Gerenciador de Grade 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 mostra quantas instâncias desse alerta estão ocorrendo em cada gravidade. **Crítico**: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. **Major**: 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 pare a operação normal de um nó ou serviço StorageGRID. **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria 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 acionado na sua hora local e em UTC. Se vários alertas forem agrupados, a linha de título mostrará horas para a instância mais recente do alerta (*newest*) e a instância mais antiga do alerta (*older*). **Alertas resolvidos**: Há quanto tempo o alerta foi acionado.
Local/nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.
Estado	Se o alerta está ativo, silenciado ou resolvido. Se vários alertas forem agrupados e **todos os alertas** estiverem selecionados na lista suspensa, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.
Tempo resolvido (apenas 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, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **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. **Nota:** se vários alertas atuais forem agrupados, os valores atuais não serão exibidos na linha de título.

Cabeçalho da coluna	Descrição
Valores acionados (apenas alertas resolvidos)	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta **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 exibir uma lista de alertas nessas categorias. Você também pode exibir os detalhes de um alerta selecionando **nós** > ***node*** > **Visão geral** e, em seguida, selecionando o alerta na tabela Alertas.

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

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

     A página de alertas atuais é atualizada a cada dois minutos.

2. Para expandir grupos de alertas, selecione o cursor para baixo . Para recolher alertas individuais num 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 os alertas atuais ou grupos de alertas, selecione as setas para cima/para baixo em cada cabeçalho de coluna.
   - Quando **alertas de grupo** é selecionado, tanto os grupos de alerta quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **tempo disparado** 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 os alertas atuais por status (**todos os alertas**, **Ativo** ou **silenciado**, use o menu suspenso na parte superior da tabela.

   "Silenciar notificações de alerta"Consulte .

6. Para classificar alertas resolvidos:
   - Selecione um período de tempo a partir do menu pendente **When Triggered**.
   - Selecione uma ou mais severidades no menu suspenso **severidade**.
   - Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **regra de alerta** para filtrar os alertas resolvidos relacionados a uma regra de alerta específica.
   - Selecione um ou mais nós no menu suspenso **Node** para filtrar os alertas resolvidos relacionados a um nó específico.

7. Para ver 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 fez com que esse alerta fosse acionado.

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

   > Tenha cuidado ao decidir silenciar uma regra de alerta. Se uma regra de alerta for silenciada, talvez você não detete um problema subjacente até que ela impeça que uma operação crítica seja concluída.

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

      Uma janela pop-up é exibida, listando a expressão Prometheus para cada gravidade definida.

   b. Para fechar o pop-up, clique em qualquer lugar fora do pop-up.
10. Opcionalmente, selecione **Editar regra** para editar a regra de alerta que fez com que esse alerta fosse acionado.

    Você deve ter o "Gerencie 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 detete um problema subjacente até que ele impeça que uma operação crítica seja concluída.

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

Monitorar a capacidade de armazenamento

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

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

Você pode "ver informações sobre a capacidade de armazenamento" fazer toda a grade, para cada local e para cada nó de storage em seu sistema StorageGRID.

Monitore a capacidade de armazenamento de toda a grade

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

O painel do Grid Manager permite avaliar rapidamente a quantidade de armazenamento 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.

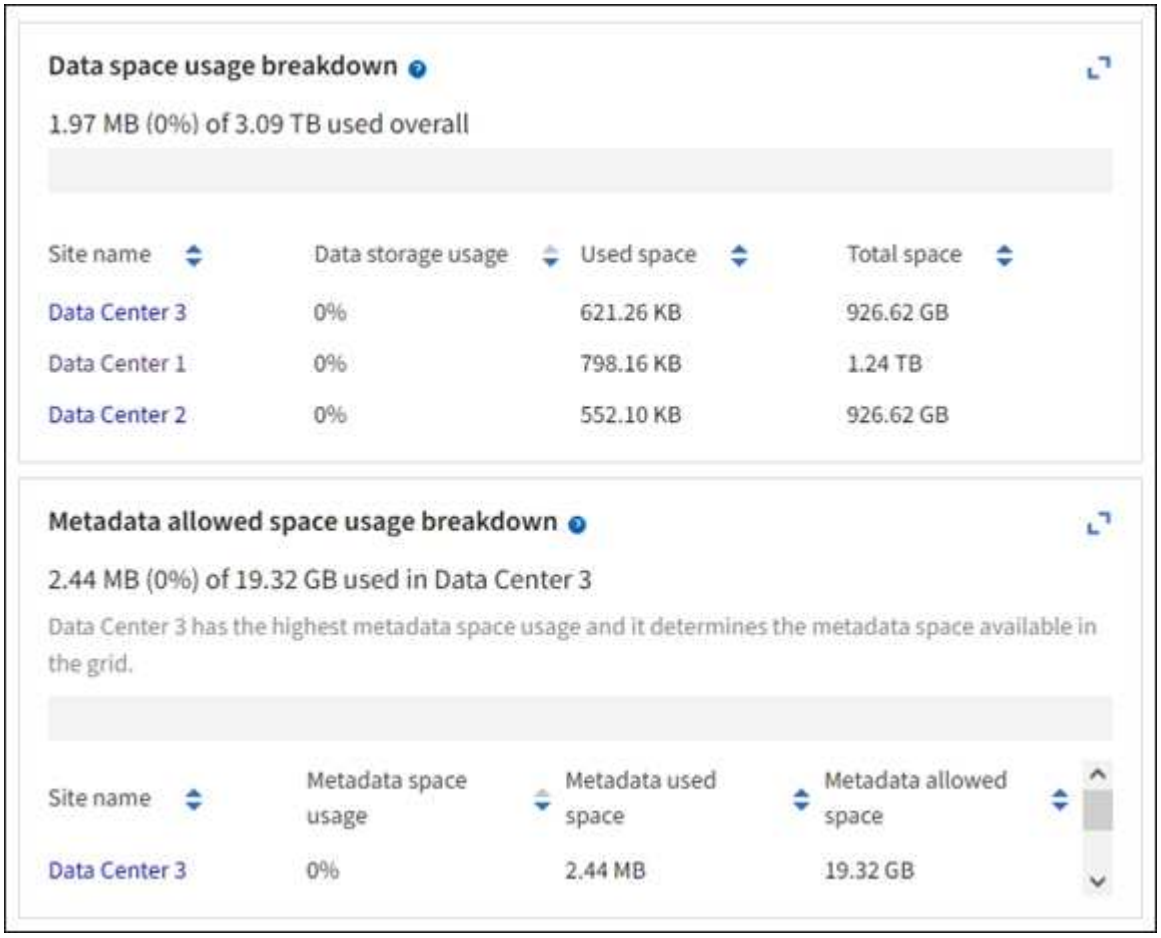
Passos

1. Avalie a quantidade de storage disponível para toda a grade e para cada data center.

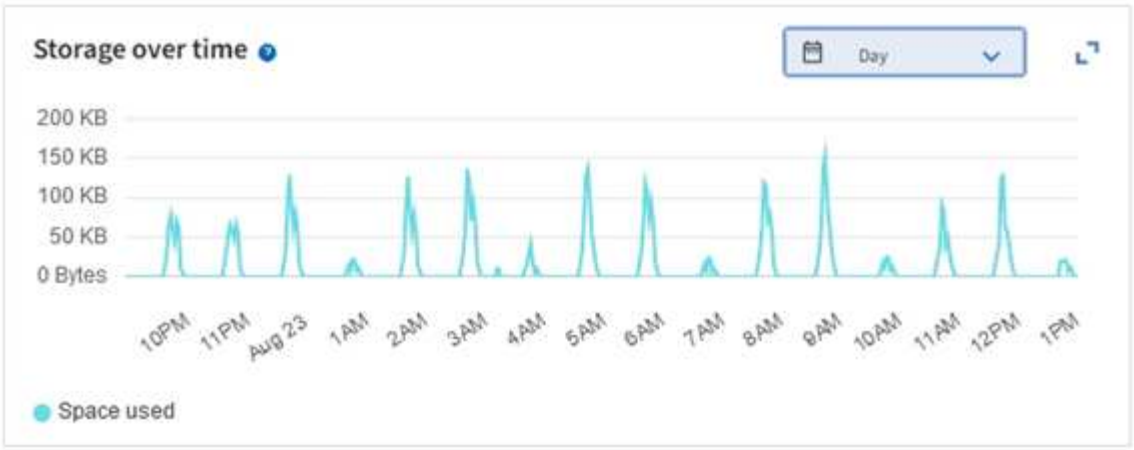
   a. Selecione **Painel > Visão geral**.

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

      O resumo não inclui Mídia de arquivamento.



   a. Observe o gráfico no cartão armazenamento ao longo do tempo. Use a lista suspensa período de tempo para ajudá-lo a determinar a rapidez com que o armazenamento é consumido.



2. Use a página nós para obter detalhes adicionais sobre quanto storage foi usado e quanto storage permanece disponível na grade para dados de objetos e metadados de objetos.
   a. Selecione **NODES**.
   b. Selecione ***Grid*** > **Storage**.

   c. Posicione o cursor sobre os gráficos **armazenamento usado - dados de objetos** e **armazenamento usado - metadados de objetos** para ver quanto armazenamento de objetos e metadados de objetos estão disponíveis para toda a grade e quanto tem sido 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 off-line.

3. Planeje realizar uma expansão para adicionar nós de storage ou volumes de storage antes que a capacidade de storage 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 usa codificação de apagamento, talvez você prefira expandir quando os nós de storage existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que precisam ser adicionados.

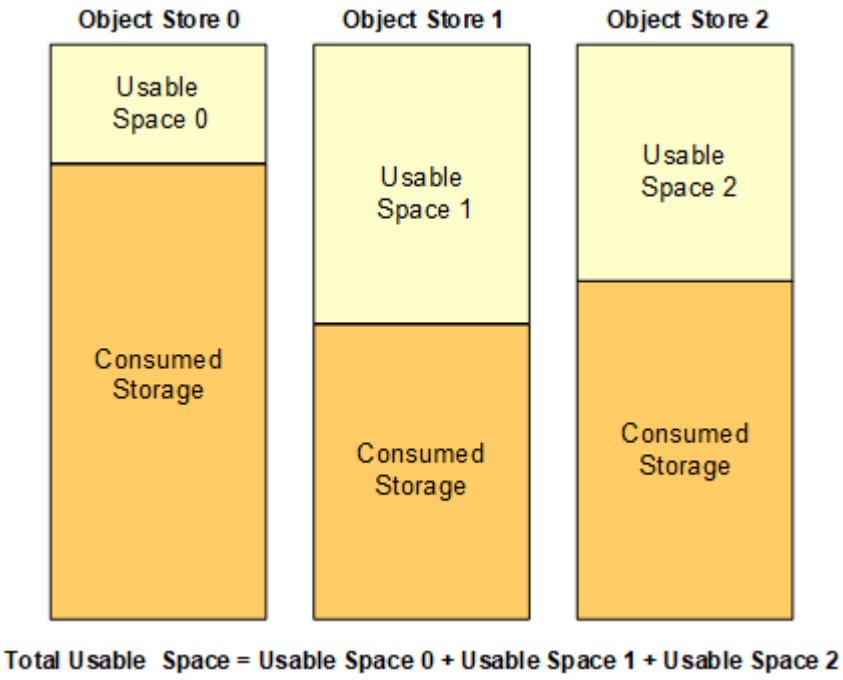
Para obter mais informações sobre como Planejar uma expansão de armazenamento, consulte o "Instruções para expandir StorageGRID".

Monitore a capacidade de storage para cada nó de storage

Monitore o espaço utilizável total para cada nó de storage 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 utilizável total para um nó de storage é calculado adicionando o espaço disponível em todos os armazenamentos de objetos dentro do nó.



Passos

1. Selecione **NÓS** > ***Storage Node*** > **Storage**.

   Os gráficos e tabelas para o nó aparecem.

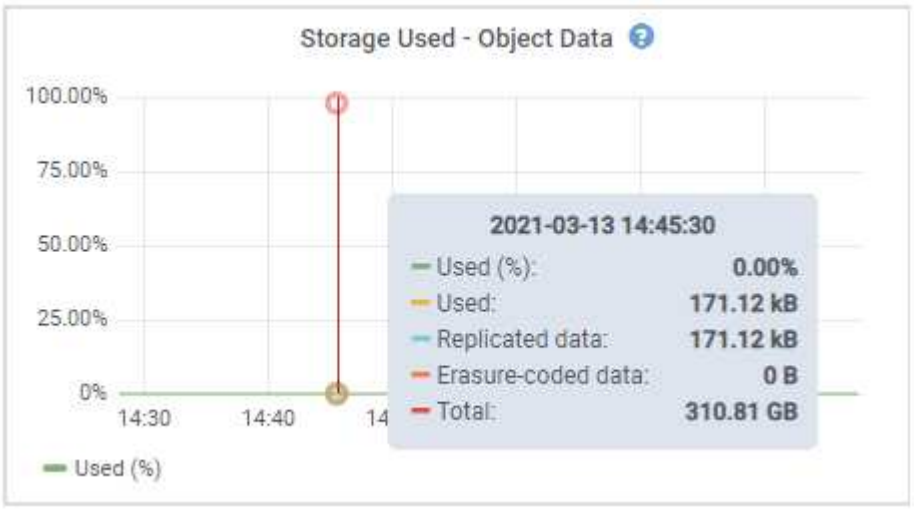
2. Posicione o cursor sobre o gráfico armazenamento usado - dados do objeto.

   São apresentados os seguintes valores:

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

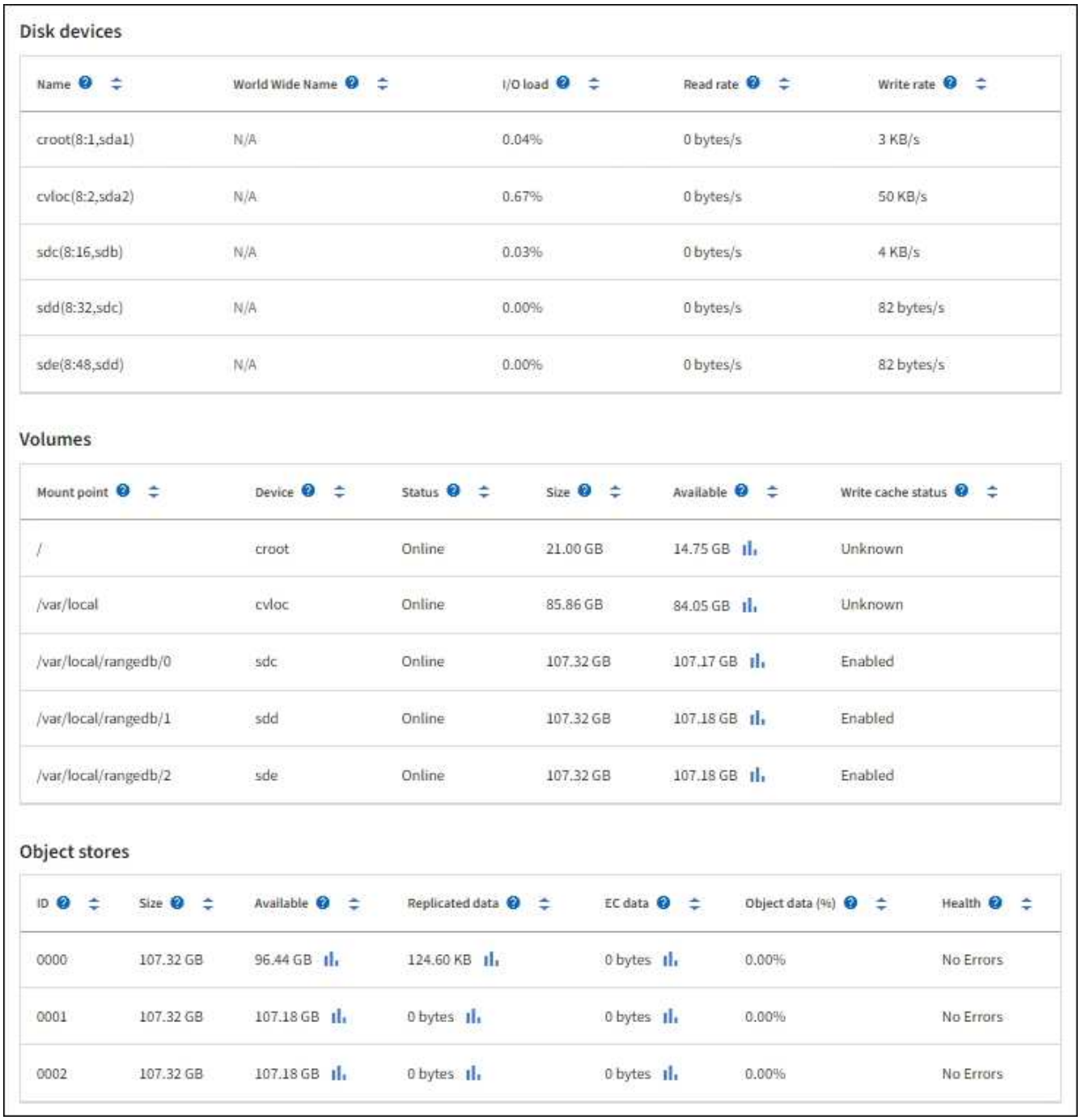
por apagamento neste nó, site ou grade.

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



3. Reveja os valores disponíveis nas tabelas volumes e objetos armazenados, abaixo dos gráficos.

Para visualizar gráficos destes valores, clique nos ícones de 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 na qual o espaço de armazenamento utilizável está sendo consumido.
5. Para manter as operações normais do sistema, adicione nós de storage, adicione volumes de storage 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 usa codificação de apagamento, talvez você prefira expandir quando os nós de storage existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que precisam ser adicionados.

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

"Instruções para expandir StorageGRID".

"Baixo armazenamento de dados de objetos"O alerta é acionado quando o espaço insuficiente permanece para armazenar dados de objetos em um nó de armazenamento.

Monitore a capacidade dos metadados de objetos para cada nó de storage

Monitore o uso de metadados para cada nó de storage para garantir que o espaço adequado permaneça disponível para operações essenciais do banco de dados. É necessário adicionar novos nós de storage em cada local antes que os metadados do objeto excedam 100% do espaço permitido dos metadados.

Sobre esta tarefa

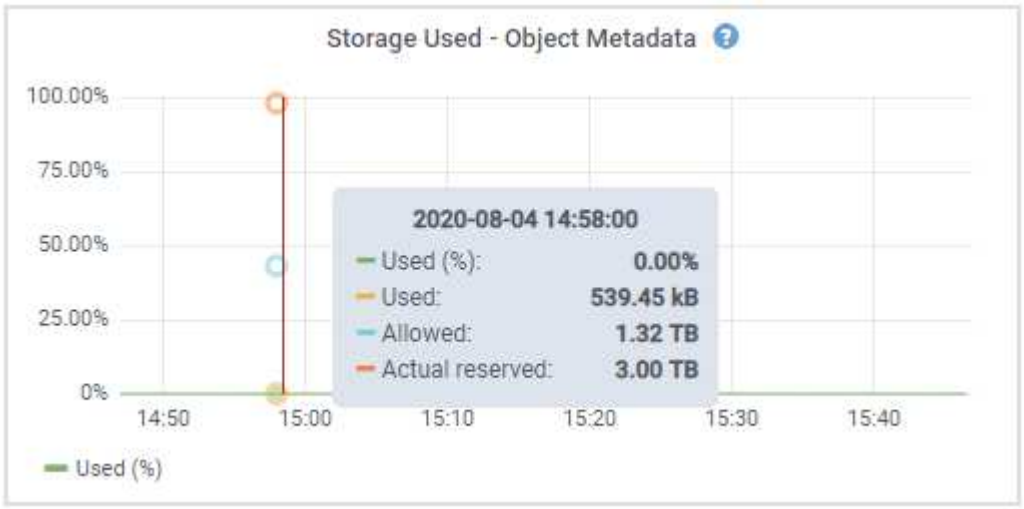
O StorageGRID mantém três cópias de metadados de objetos em cada local para fornecer redundância e proteger os metadados de objetos da perda. As três cópias são distribuídas uniformemente por todos os nós de storage em cada local, usando o espaço reservado para metadados no volume de storage 0 de cada nó de storage.

Em alguns casos, a capacidade de metadados de objetos da grade pode ser consumida mais rápido do que sua capacidade de armazenamento de objetos. Por exemplo, se você costuma ingerir um grande número de objetos pequenos, talvez seja necessário adicionar nós de storage para aumentar a capacidade dos metadados, mesmo que haja capacidade suficiente de storage de objetos.

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 peças em um upload de várias partes e a frequência de alterações nos locais de armazenamento de ILM.

Passos

1. Selecione **NÓS** > ***Storage Node*** > **Storage**.
2. Posicione o cursor sobre o gráfico armazenamento usado - metadados de objetos para ver os valores de um tempo específico.



Usado (%)

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

Métricas de 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 Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

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

Métrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Real reservado

O espaço real reservado para metadados neste nó de storage. 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 "Descrição completa do espaço reservado real para metadados".

Prometheus métrica 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 off-line.

3. Se o valor **usado (%)** for 70% ou mais, expanda o sistema StorageGRID adicionando nós de storage a cada local.

O alerta **armazenamento de metadados baixo** é acionado quando o valor **usado (%)** atinge determinados limites. Resultados indesejáveis podem ocorrer se os metadados de objetos usarem mais de 100% do espaço permitido.

Quando você adiciona os novos nós, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de storage no local. Consulte "Instruções para expandir um sistema StorageGRID".

Monitorar previsões de uso de espaço

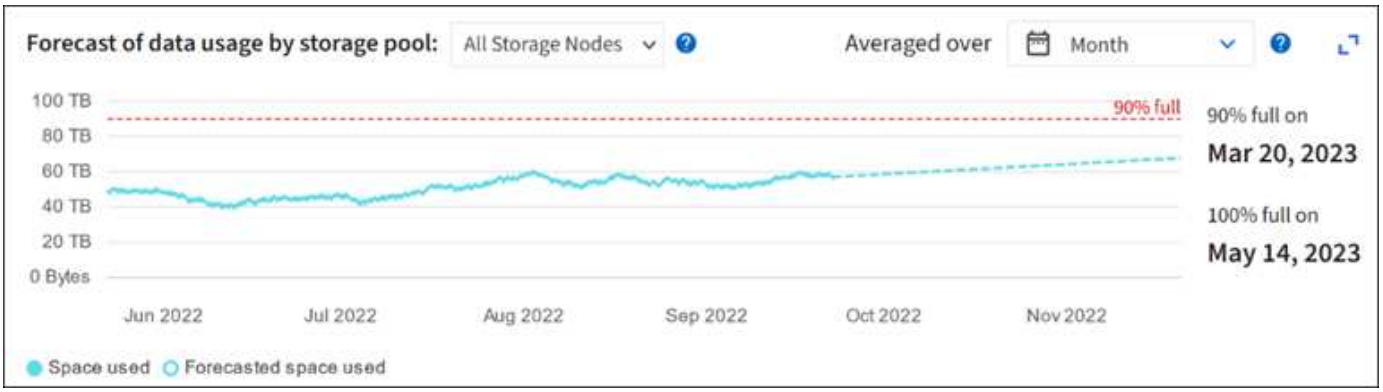
Monitore as previsões de uso de espaço para dados e metadados do usuário para estimar quando será "expanda uma grade"necessário .

Se você notar que a taxa de consumo muda ao longo do tempo, selecione um intervalo mais curto a partir da lista suspensa **Average over** (média) para refletir apenas os padrões de ingestão mais recentes. Se notar padrões sazonais, selecione um intervalo mais longo.

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 de instrumentos, selecione **armazenamento**.
2. Visualize as placas do painel, a previsão do uso de dados por pool de armazenamento e a previsão do uso de metadados por local.
3. Use esses valores para estimar quando será necessário adicionar novos nós de storage para storage de dados e metadados.



Monitorar o gerenciamento do ciclo de vida das informações

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

Sobre esta tarefa

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

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 queue objetos cujas instruções de posicionamento do ILM não possam ser cumpridas em tempo quase real. Você deve monitorar se o StorageGRID está acompanhando as ações do cliente.

Use a guia Painel do Gerenciador de Grade

Passos

Use a guia ILM no painel do Gerenciador de Grade para monitorar as operações do ILM:

1. Faça login no Gerenciador de Grade.
2. No painel, selecione a guia ILM e anote os valores no cartão de fila ILM (objetos) e no cartão de taxa de avaliação ILM.

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

Use a página NÓS

Passos

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

> Os gráficos na página **NODES** serão substituídos pelas placas de painel correspondentes em uma versão futura do StorageGRID.

1. Selecione **NODES**.
2. Selecione ***grid name*** > **ILM**.
3. Posicione o cursor sobre o gráfico de fila ILM para ver o valor dos seguintes atributos em um determinado ponto no tempo:
   - **Objetos enfileirados (das operações do cliente)**: O número total de objetos aguardando avaliação ILM devido às operações do cliente (por exemplo, ingest).
   - **Objetos enfileirados (de todas as operações)**: O número total de objetos aguardando avaliação ILM.
   - **Taxa de digitalização (objetos/seg)**: A taxa na qual os objetos na grade são digitalizados e enfileirados para ILM.
   - **Taxa de avaliação (objetos/seg)**: A taxa atual na qual os objetos estão sendo avaliados em relação à política ILM na grade.
4. Na seção fila de ILM, observe os seguintes atributos.

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

   - **Período de digitalização - estimado**: O tempo estimado para concluir uma varredura ILM completa de todos os objetos.

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

   - **Tentativas de reparação**: O número total de operações de reparação de objetos para dados replicados que foram tentados. Essa contagem aumenta cada vez que um nó de storage tenta reparar um objeto de alto risco. As reparações ILM de alto risco são priorizadas se a grelha ficar ocupada.

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

   Esses atributos podem ser úteis quando você está monitorando o progresso da recuperação do volume do nó de armazenamento. Se o número de reparações tentadas tiver parado de aumentar e tiver sido concluído um exame completo, a reparação provavelmente foi concluída.

Monitorar recursos de rede e do sistema

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

Monitorar conexões de rede e desempenho

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

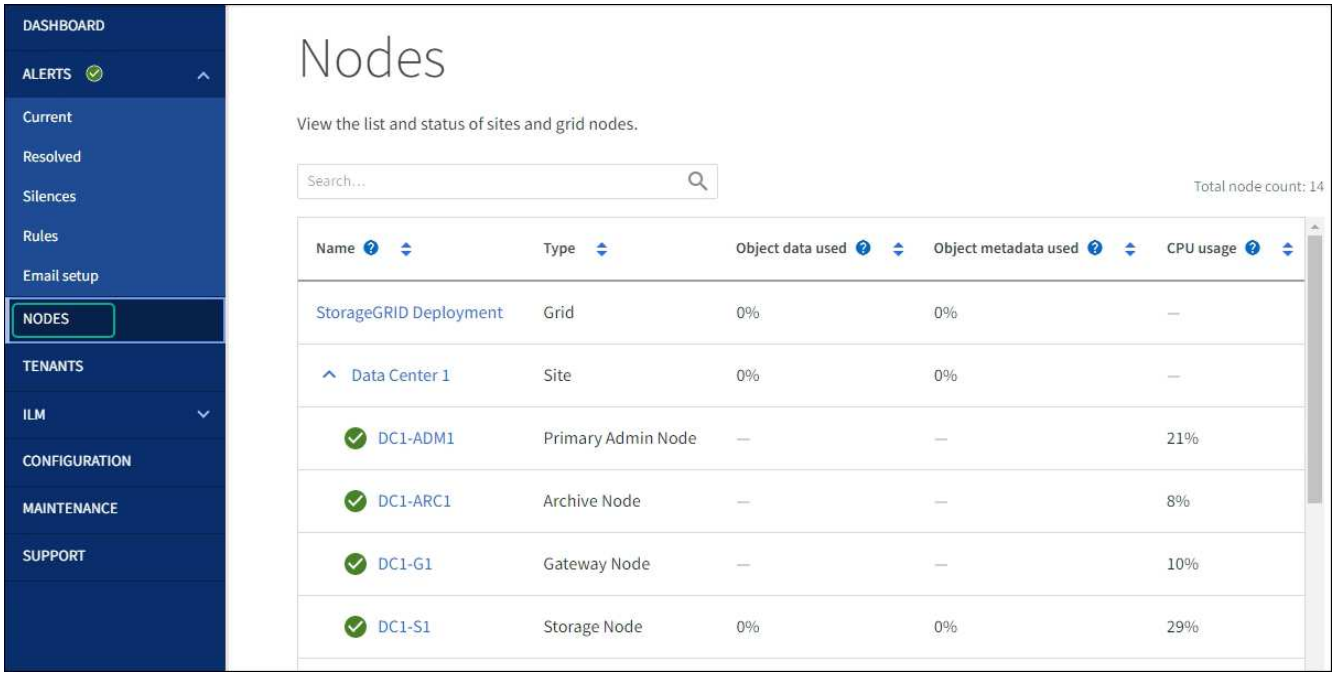
Use o Gerenciador de Grade para monitorar a conetividade e o desempenho da rede, para que você possa resolver quaisquer problemas imediatamente.

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

Passos

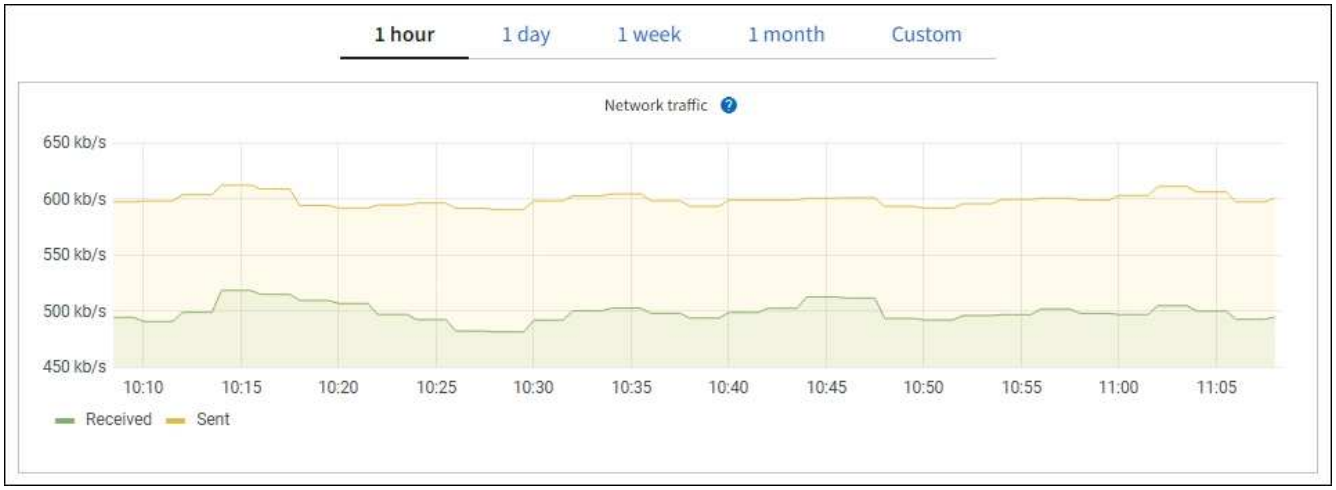
1. Selecione **NODES**.

   A página nós é exibida. Cada nó na grade é listado no formato de tabela.

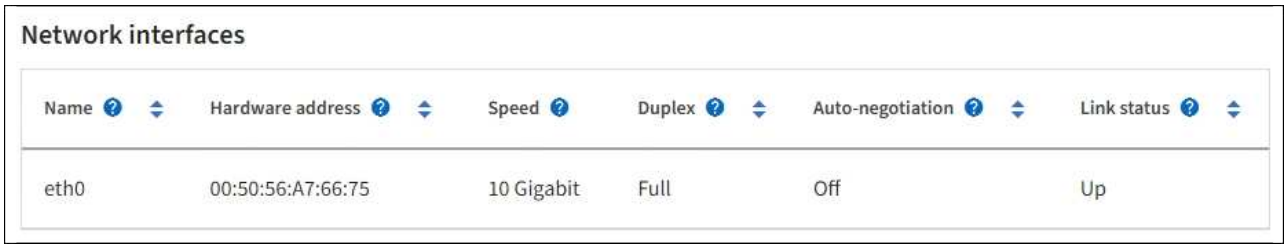


2. Selecione o nome da grade, um site específico de data center ou um nó de grade e, em seguida, selecione a guia **rede**.

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

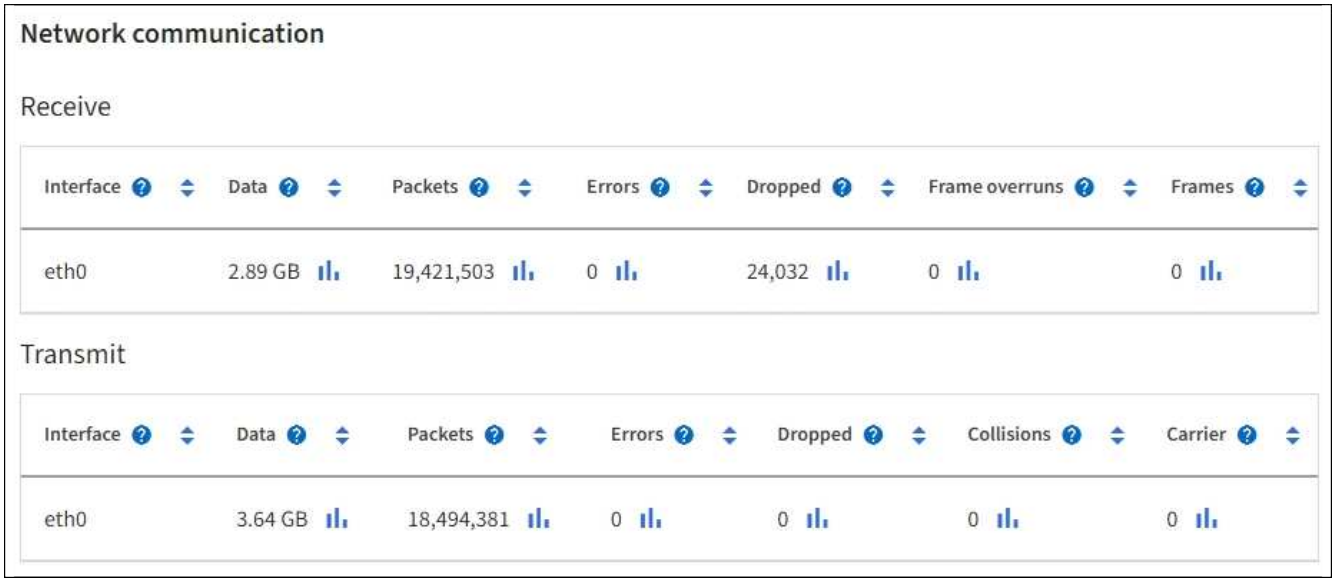


   a. Se você selecionou um nó de grade, role para baixo para revisar a seção **interfaces de rede** da página.



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

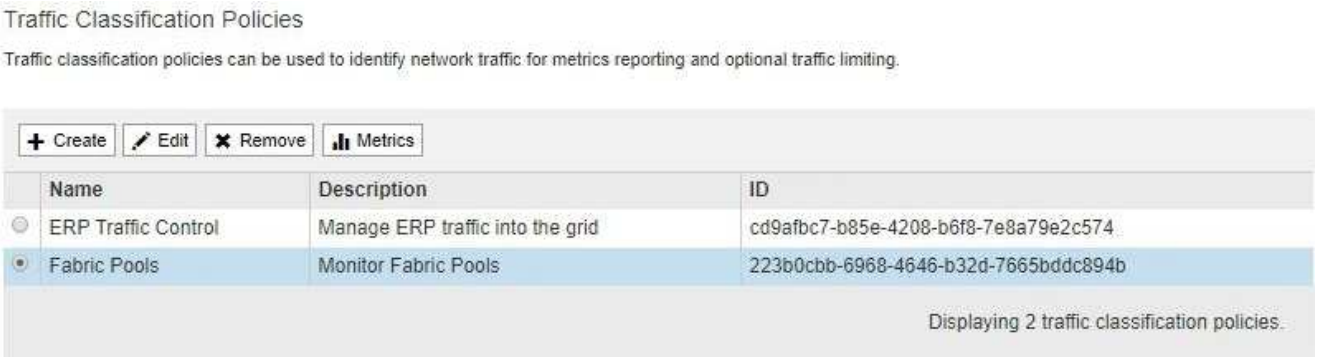
As tabelas de receção e transmissão mostram quantos bytes e pacotes foram recebidos e enviados através de cada rede, bem como outras métricas de receção e transmissão.



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

a. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.

A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.



a. Para exibir 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. Reveja os gráficos para compreender o tráfego de rede associado à política.

Se uma política de classificação de tráfego for projetada para limitar o tráfego de rede, analise a frequência com que 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

"Veja a guia rede"

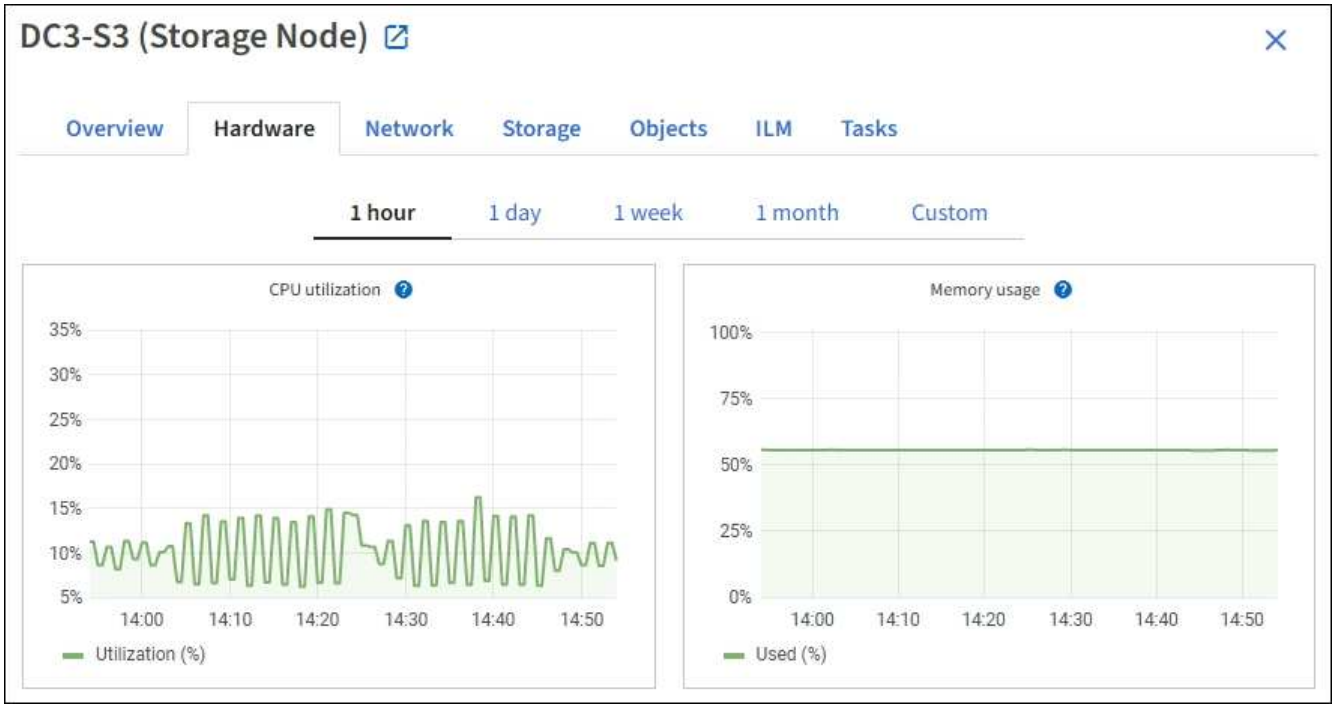
"Monitorar os estados de conexão do nó"

Monitore os recursos no nível do nó

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

Passos

1. Na página **NÓS**, selecione o nó.
2. Selecione a guia **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 ou 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 em um dispositivo de serviços, role para baixo para exibir as tabelas de componentes. O estado de todos os componentes deve ser "nominal". Investigue componentes que tenham qualquer outro estado.

Informações relacionadas

"Exibir informações sobre os nós de storage do dispositivo"

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

Monitorar a atividade do locatário

Todas as atividades dos clientes S3 e Swift estão associadas às contas de inquilino do

StorageGRID. Você pode usar o Gerenciador de Grade para monitorar o uso do 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 reunir informações mais detalhadas sobre como os locatários estão usando o StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Acesso root ou permissão de contas do locatário".

Ver todos os inquilinos

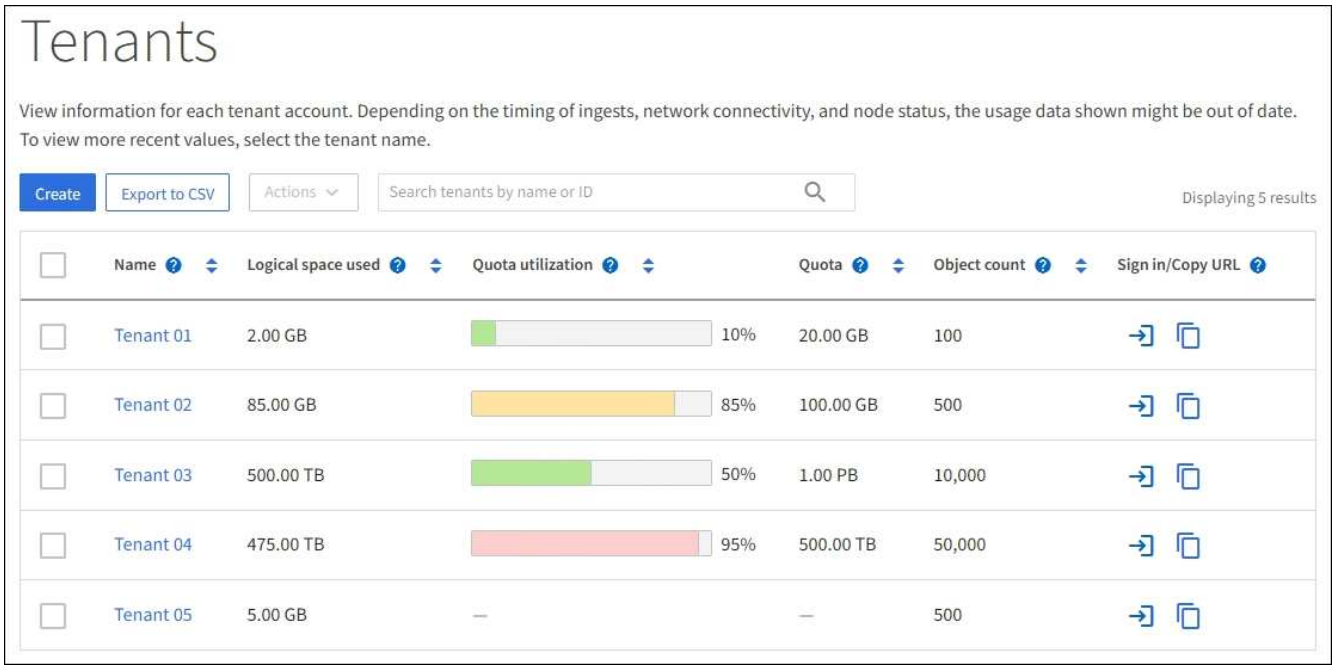
A página inquilinos mostra informações básicas para todas as contas de inquilino atuais.

Passos

1. Selecione **TENANTS**.
2. Reveja as informações apresentadas nas páginas do locatário.

   O espaço lógico usado, a utilização 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 utilização da cota e quota contêm um traço (& n.o 8212;).

   Os valores de espaço utilizados são estimativas. Essas estimativas são afetadas pelo timing de inests, conetividade de rede e status de nó.



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

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

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

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` arquivo 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. "Eliminar conta de inquilino"Consulte .

   Não é possível remover uma conta de locatário se a conta incluir quaisquer buckets ou contentores.

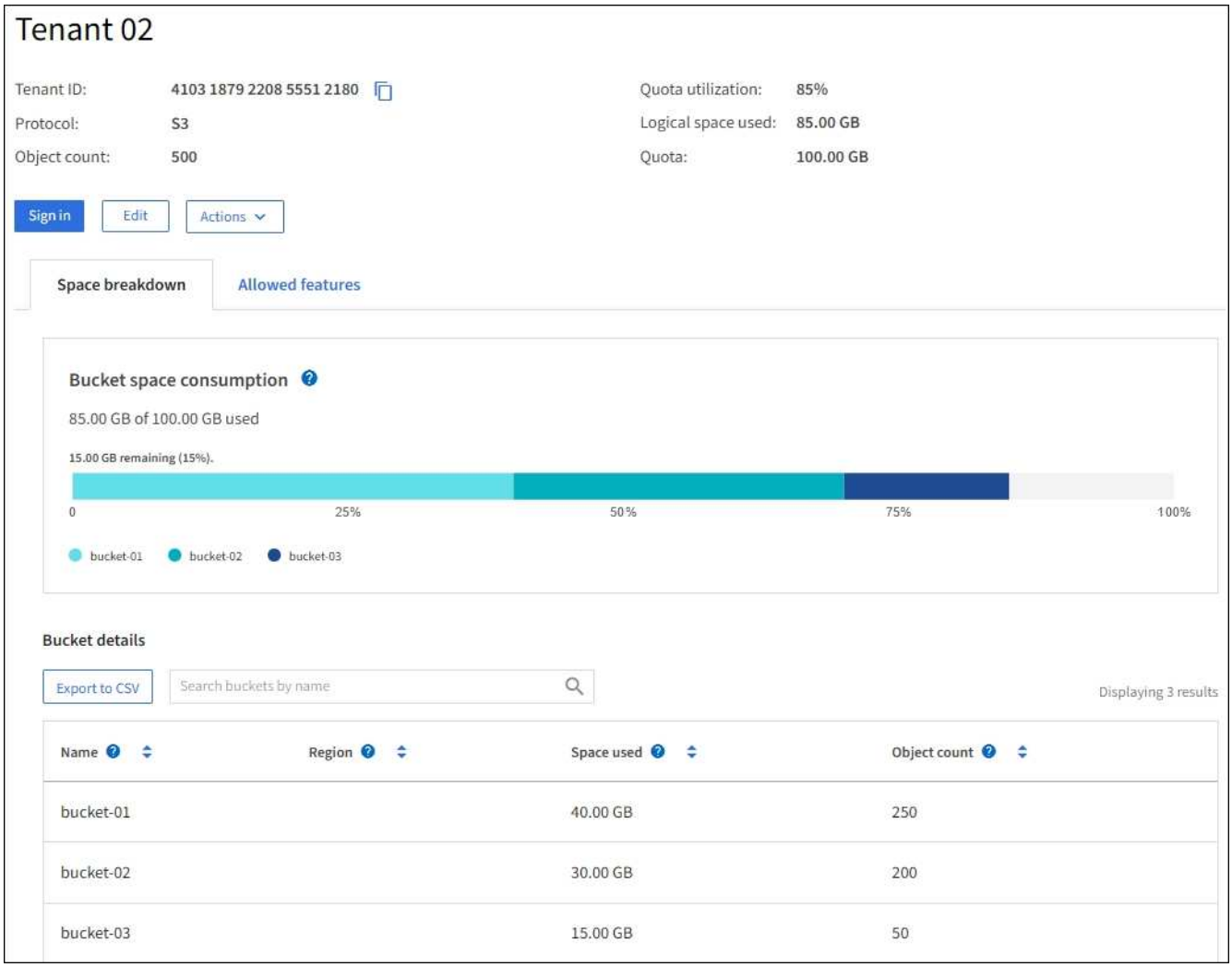
Exibir um locatário específico

Você pode exibir detalhes de um locatário específico.

Passos

1. Selecione o nome do locatário na página de locatários.

   A página de detalhes do locatário é exibida.



2. Revise a visão geral do locatário na parte superior da página.

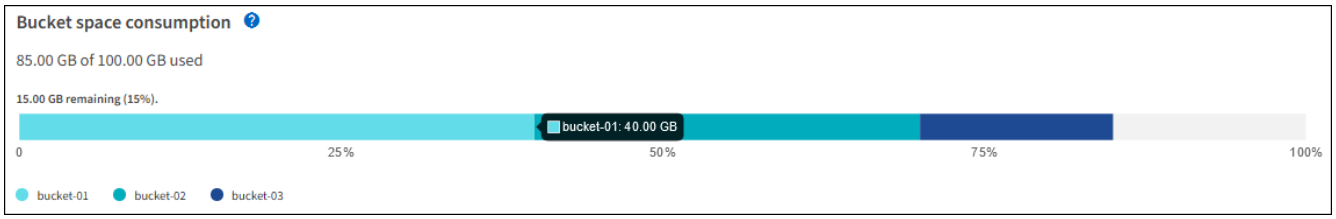
   Esta seção da página de detalhes fornece informações resumidas para o locatário, incluindo a contagem de objetos do locatário, a utilização da cota, o espaço lógico usado e a configuração da cota.

3. Na guia **repartição de espaço**, revise o gráfico **consumo de espaço**.

   Este gráfico mostra o consumo total de espaço para todos os buckets do S3 do locatário (ou contentores Swift).

   Se uma cota foi definida para esse locatário, a quantidade de cota usada e restante será exibida no 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 usada (por exemplo, `85.00 GB used`). O gráfico de barras mostra a porcentagem de cota em cada bucket ou contentor. Se o inquilino tiver excedido a cota de armazenamento em mais de 1% e em pelo menos 1 GB, o gráfico mostrará a cota total e a quantidade excedente.

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



A utilização de quotas baseia-se em estimativas internas e pode ser ultrapassada em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novos ingere se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em conta 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 a utilização da cota seja recalculada. Os cálculos de utilização de cotas podem levar 10 minutos ou mais.

A utilização da cota de um locatário indica a quantidade total de dados de objeto que o locatário carregou para o StorageGRID (tamanho lógico). A utilização da cota não representa o espaço usado para armazenar cópias desses objetos e seus metadados (tamanho físico).

Você pode ativar a regra de alerta **uso de cota de locatário alta** para determinar se os locatários estão consumindo suas cotas. Se ativado, esse alerta é acionado quando um locatário usou 90% de sua cota. Para obter instruções, "Editar regras de alerta"consulte .

4. Na guia **quebra de espaço**, revise os **Detalhes do balde**.

   Esta tabela lista os buckets S3 (ou contentores Swift) para o locatário. O espaço usado é a quantidade total de dados de objetos no bucket ou no contêiner. Esse valor não representa o espaço de storage necessário para cópias do ILM e metadados de objetos.

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

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

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` arquivo em um aplicativo de Planilha ou usá-lo em automação.

6. Opcionalmente, selecione a guia **recursos permitidos** para ver uma lista das permissões e recursos que estão habilitados para o locatário. "Editar conta de locatário"Veja se você precisa 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.

   "O que é a federação de grade?"Consulte e "Gerenciar os locatários permitidos para a federação de grade".

Ver o tráfego de rede

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

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.

   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 as que se aplicam a um locatário específico.
3. Para exibir 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 ajustar a política.

Consulte "Gerenciar políticas de classificação de tráfego" para obter mais informações.

Use o log de auditoria

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

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

- Operações específicas do cliente, como COLOCAR, OBTER ou EXCLUIR
- 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 log escolhida. Isso permite que você entenda melhor as atividades do cliente ou implemente modelos sofisticados de chargeback e cobrança.

Consulte "Rever registos de auditoria" para obter mais informações.

Use métricas Prometheus

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

- No Gerenciador de Grade, selecione **support** > **Tools** > **Metrics**. Você pode usar painéis existentes, como a Visão geral do S3, para analisar as atividades do cliente.

  > As ferramentas disponíveis na página Metrics destinam-se principalmente ao uso pelo suporte técnico. Alguns recursos e itens de menu dentro dessas ferramentas são intencionalmente não funcionais.

- Na parte superior do Gerenciador de Grade, 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 personalizadas e painéis para a atividade do locatário.

Consulte "Analise as métricas de suporte" para obter mais informações.

Monitore as operações dos clientes S3 e Swift

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

Antes de começar

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

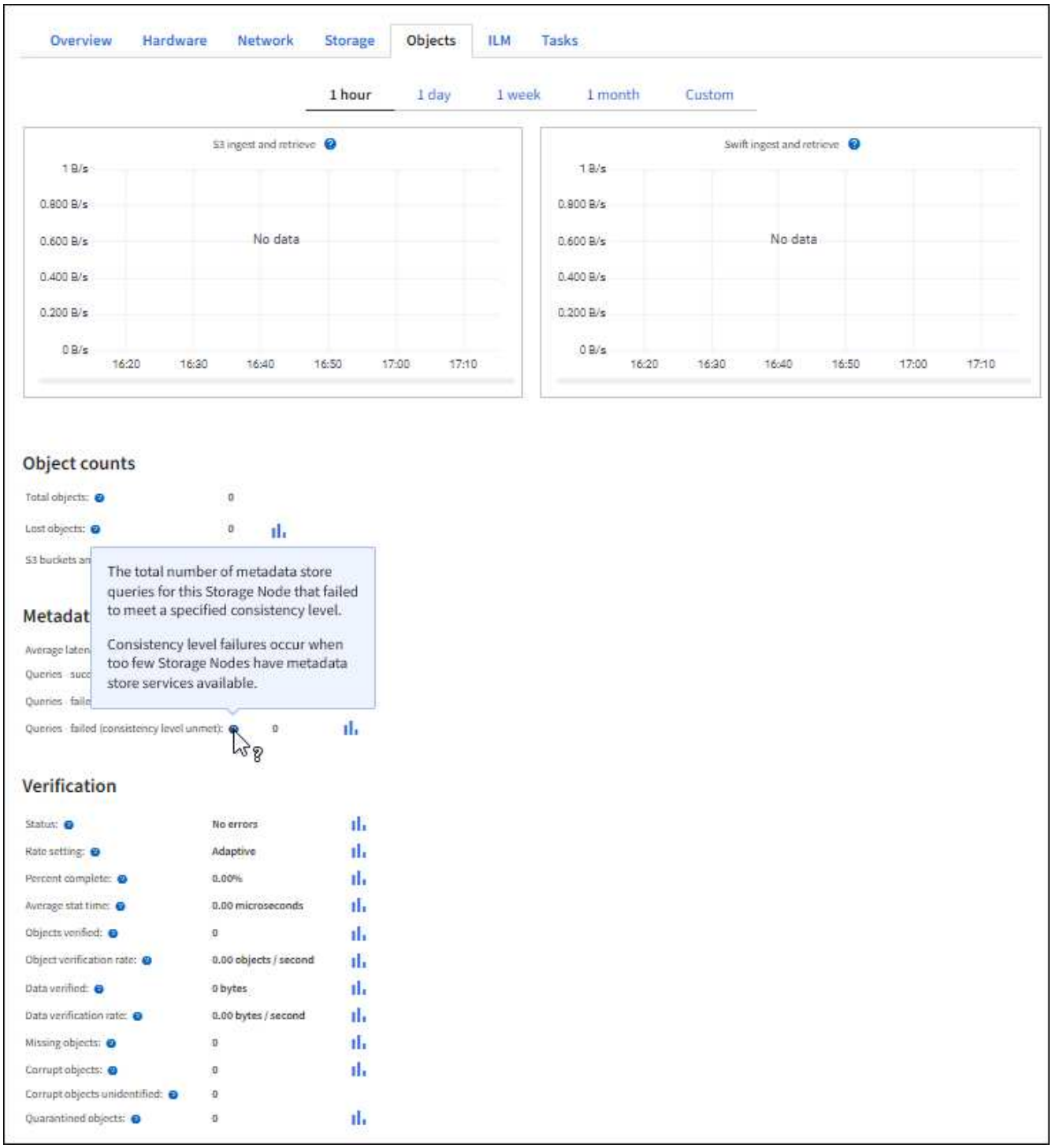
Passos

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

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

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

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



Monitorar operações de balanceamento de carga

Se você estiver usando um balanceador de carga para gerenciar conexões de cliente com o StorageGRID, monitore as operações de balanceamento de carga após configurar o sistema inicialmente e depois de fazer alterações 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 storage.

Depois de configurar o balanceamento de carga, você deve confirmar que as operações de obtenção e recuperação de objetos estão sendo distribuídas uniformemente pelos nós de storage. As solicitações distribuídas uniformemente garantem que o StorageGRID permaneça responsivo às solicitações do cliente sob carga e possa ajudar a manter o desempenho do cliente.

Se você configurou um grupo de alta disponibilidade (HA) de nós de Gateway ou nós de administrador no modo de backup ativo, apenas um nó no grupo distribui ativamente as solicitações de cliente.

Para obter mais informações, "Configurar conexões de cliente S3 e Swift"consulte .

Passos

1. Se os clientes S3 ou Swift se conetarem usando o serviço Load Balancer, verifique se os nós Admin ou os nós de Gateway estão distribuindo ativamente o tráfego como você espera:
   a. Selecione **NODES**.
   b. Selecione um nó de gateway ou nó de administrador.
   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.

      Os nós com a função de primário e nós que não estão em um grupo de HA devem estar distribuindo ativamente solicitações aos clientes.

   d. Para cada nó que deve estar distribuindo ativamente solicitações de cliente, selecione o "Separador Load Balancer (carregar balanceador)".
   e. Revise o gráfico de tráfego de solicitação do Load Balancer para a última semana para garantir que o nó esteja distribuindo solicitações ativamente.

      Os nós de 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 cliente.

   f. Revise o gráfico da taxa de solicitação de entrada do Load Balancer da última semana para analisar a taxa de transferência de objetos do nó.
   g. Repita estas etapas para cada nó de administrador ou nó de gateway no sistema StorageGRID.
   h. Opcionalmente, use políticas de classificação de tráfego para visualizar uma análise mais detalhada do tráfego que está sendo servido pelo serviço Load Balancer.
2. Verifique se essas solicitações estão sendo distribuídas uniformemente para os nós de storage.
   a. Selecione ***Storage Node*** > **LDR** > **HTTP**.
   b. Reveja 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 storage.

Monitorar conexões de federação de grade

Você pode monitorar informações básicas sobre todas "conexões de federação de grade", informações detalhadas sobre uma conexão específica ou métricas do Prometheus sobre operações de replicação entre grades. Você pode monitorar uma conexão de qualquer grade.

Antes de começar

- Você está conetado ao Gerenciador de Grade em qualquer grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz" para a grade na qual você está conetado.

Ver todas as ligações

A página de 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

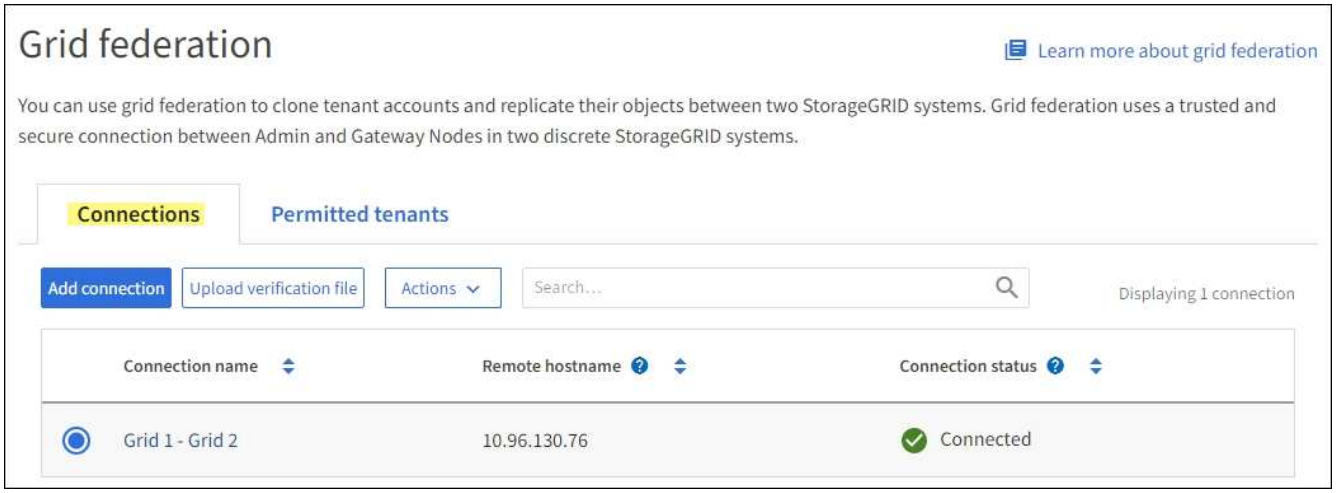
1. Selecione **CONFIGURATION** > **System** > **Grid Federation**.

   A página de federação de grade é exibida.

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

   Nesta guia, você pode:

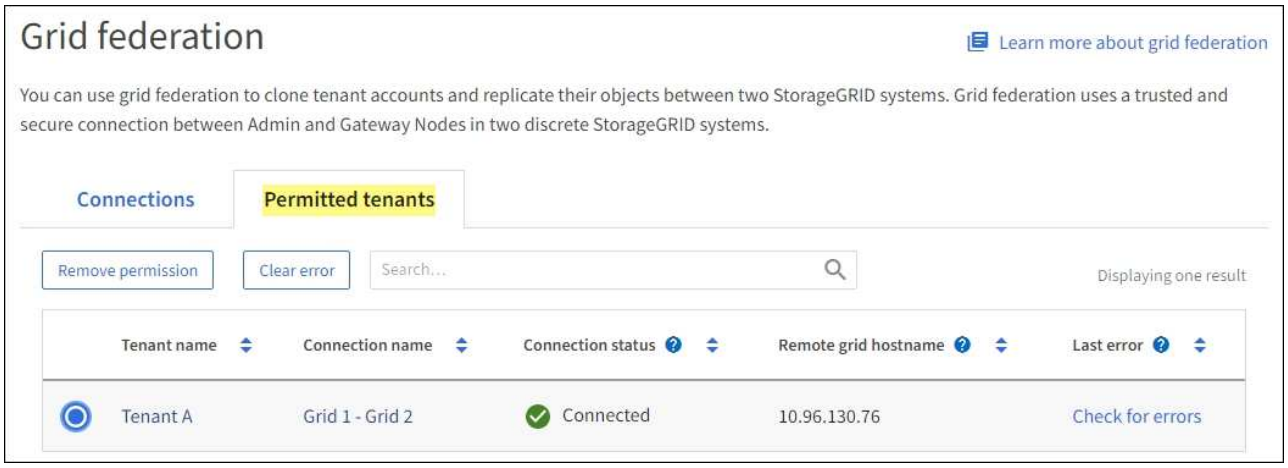
   - "Crie uma nova conexão".
   - Selecione uma conexão existente com "editar ou testar"o .



3. Para ver as informações básicas de todas as contas de inquilino nesta grade que têm a permissão **Use Grid Federation Connection**, selecione a guia **allowed tenants**.

   Nesta guia, você pode:

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



Veja uma conexão específica

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

Passos

1. Selecione qualquer guia na página de federação de Grade e selecione o nome da conexão na tabela.

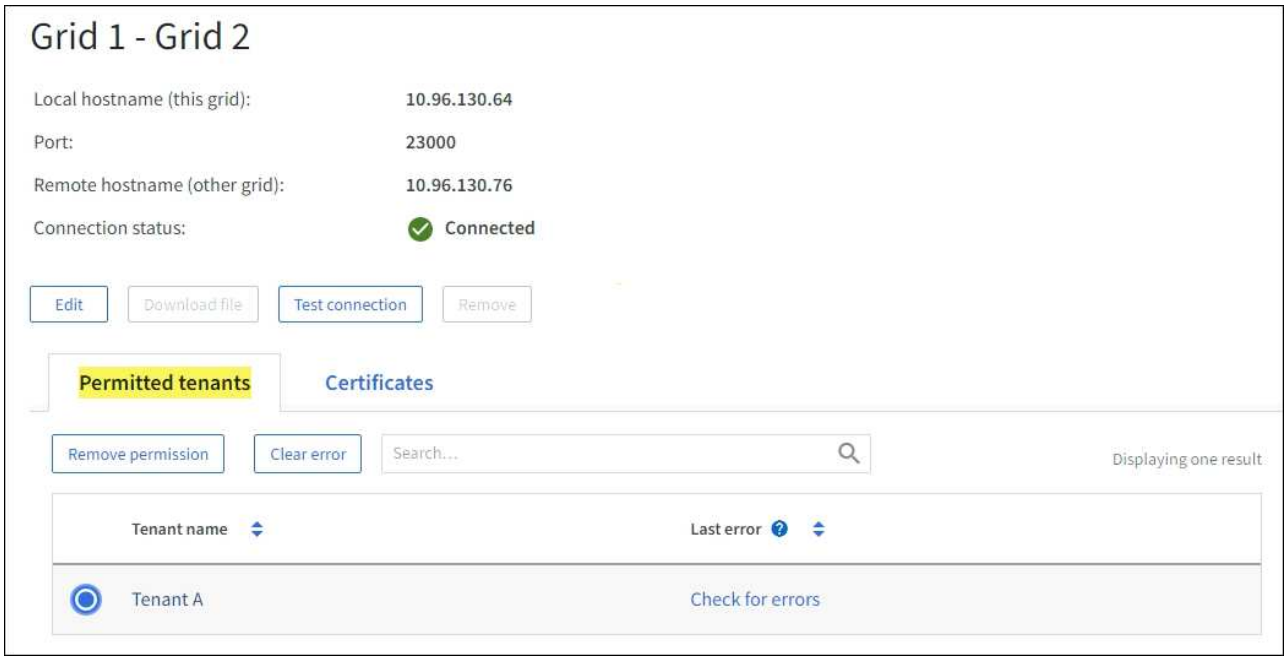
   Na página de detalhes da conexão, você pode:

   - Consulte informações básicas de status sobre a conexão, incluindo nomes de host locais e remotos, porta e status da conexão.
   - Selecione uma ligação ao "edite, teste ou remova".

2. Ao visualizar uma conexão específica, selecione a guia **allowed tenants** (inquilinos permitidos) para exibir detalhes sobre os locatários permitidos para a conexão.

   Nesta guia, você pode:

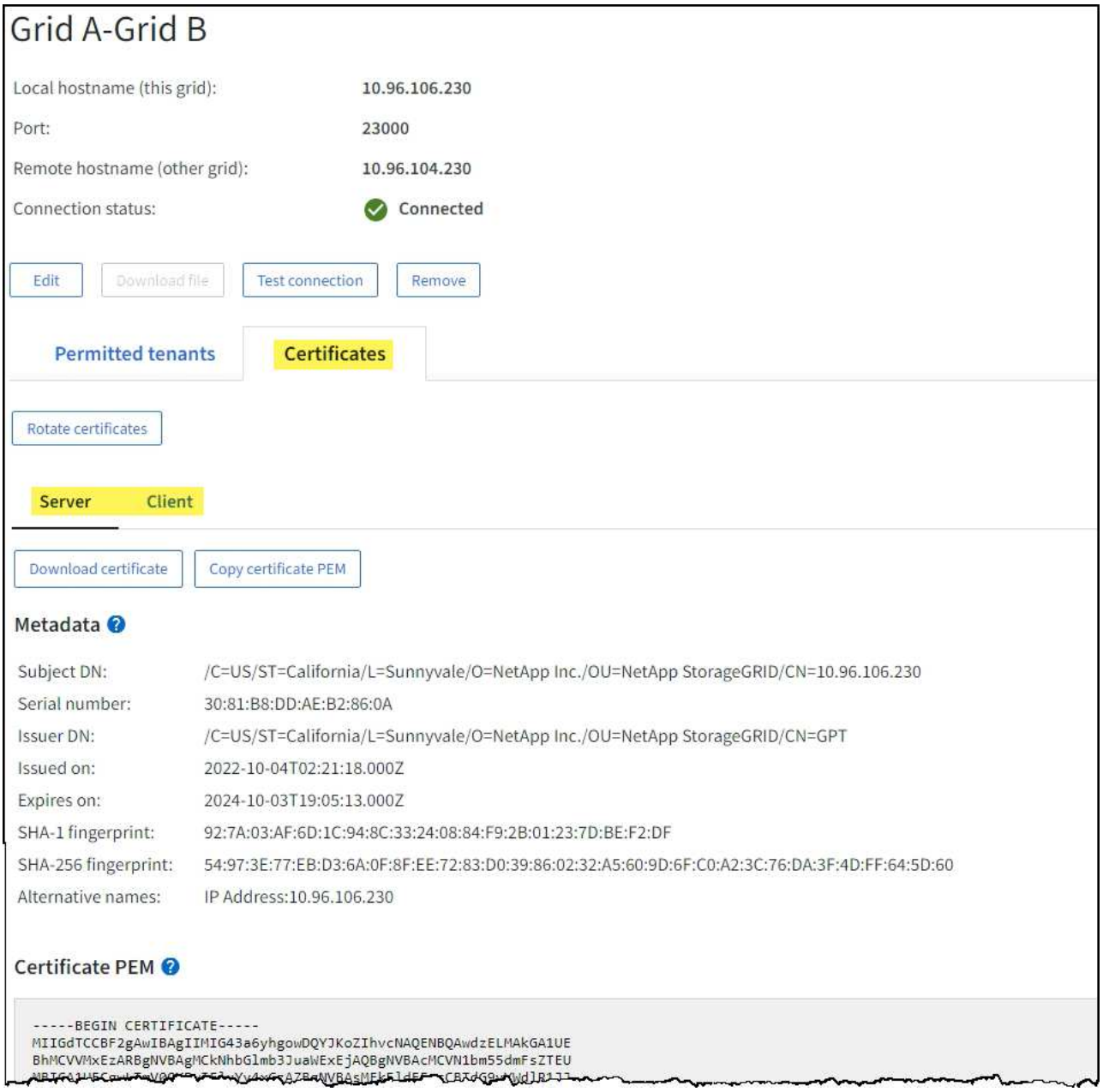
   - "Veja a página de detalhes de cada locatário permitido".
   - "Remova a permissão de um locatário" para utilizar a ligação.
   - Verifique se há erros de replicação entre redes e limpe o último erro. "Solucionar erros de federação de grade"Consulte .



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

   Nesta guia, você pode:

   - "Rode os certificados de ligação".
   - Selecione **Server** ou **Client** para visualizar ou baixar o certificado associado ou copiar o PEM do certificado.



Analise as métricas de replicação entre grades

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

Passos

1. No Gerenciador de Grade, selecione **support** > **Tools** > **Metrics**.

> As ferramentas disponíveis na página Metrics destinam-se a ser utilizadas pelo suporte técnico. Alguns recursos e itens de menu dentro dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Consulte a lista "Métricas de Prometheus comumente usadas"de .

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

   Para obter instruções detalhadas, "Analise as métricas de suporte"consulte .

3. Para repetir a replicação de objetos que não conseguiram replicar, "Identificar e tentar novamente operações de replicação com falha"consulte .

Monitorar a capacidade de arquivamento

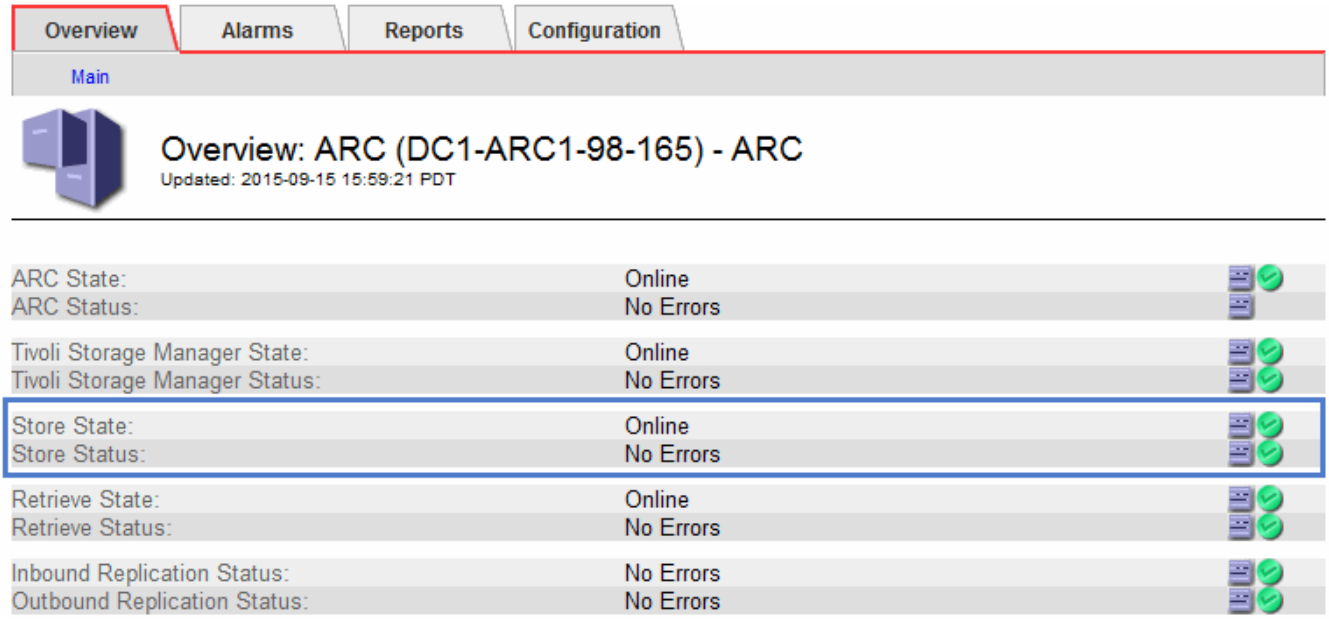
Não é possível monitorar diretamente a capacidade de um sistema de armazenamento de arquivamento externo por meio do sistema StorageGRID. No entanto, você pode monitorar se o nó Arquivo ainda pode enviar dados de objeto para o destino do arquivamento, o que pode indicar que uma expansão de Mídia de arquivamento é necessária.

Sobre esta tarefa

Você pode monitorar o componente armazenar para verificar se o nó de arquivo ainda pode enviar dados de objeto para o sistema de armazenamento de arquivamento de destino. O alarme de falhas de armazenamento (ARVF) também pode indicar que o sistema de armazenamento de arquivos visado atingiu a capacidade e não pode mais aceitar dados de objetos.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC> Overview> Main**.
3. Verifique os atributos Estado da Loja e Estado da Loja para confirmar se o componente da Loja está Online sem erros.



Um componente de armazenamento offline ou um com erros pode indicar que o sistema de armazenamento de arquivos de destino não pode mais aceitar dados de objeto porque atingiu a capacidade.

Alertas e alarmes

Gerenciar alertas e alarmes: Visão geral

O sistema de alerta StorageGRID foi concebido para o informar sobre problemas

operacionais que requerem a sua atenção. O sistema de alarme legado está obsoleto.

Sistema de alerta

O sistema de alerta foi concebido para ser a sua principal ferramenta para monitorizar quaisquer problemas que possam ocorrer no seu sistema StorageGRID. O sistema de alerta fornece uma interface fácil de usar para detetar, avaliar e resolver problemas.

Os alertas são acionados em níveis de gravidade específicos quando as condições das regras de alerta são consideradas verdadeiras. Quando um alerta é acionado, ocorrem as seguintes ações:

- Um ícone de gravidade de alerta é mostrado no painel do Gerenciador de Grade e a contagem de Alertas atuais é incrementada.
- O alerta é mostrado na página de resumo **NÓS** e na guia **NÓS** > ***node*** > **Visão geral**.
- 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 SNMP (Simple Network Management Protocol) é enviada, supondo que você tenha configurado o agente SNMP do StorageGRID.

Sistema de alarme legado

Como alertas, os alarmes são acionados em níveis específicos de gravidade quando os atributos atingem valores de limite definidos. No entanto, ao contrário dos alertas, muitos alarmes são acionados para eventos que você pode ignorar com segurança, o que pode resultar em um número excessivo de notificações de e-mail ou SNMP.

> O sistema de alarme está obsoleto e será removido em uma versão futura. Se você ainda estiver usando alarmes herdados, você deve fazer a transição completa para o sistema de alerta o mais rápido possível.

Quando um alarme é acionado, ocorrem as seguintes acões:

- O alarme aparece na página **SUPPORT** > **Alarmes (legacy)** > **current Alarms** (alarmes atuais).
- Uma notificação por e-mail é enviada, supondo que você tenha configurado um servidor SMTP e configurado uma ou mais listas de e-mail.
- Uma notificação SNMP pode ser enviada, supondo que você tenha configurado o agente SNMP do StorageGRID. (As notificações SNMP não são enviadas para todos os alarmes ou gravidades de alarme.)

Compare alertas e alarmes

Existem várias semelhanças entre o sistema de alerta e o sistema de alarme antigo, mas o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Consulte a tabela a seguir para saber como executar operações semelhantes.

	Alertas	Alarmes (sistema legado)
Como posso ver quais alertas ou alarmes estão ativos?	• Selecione o link **Current alerts** no painel. • Selecione o alerta na página **NODES** > **Overview**. • Selecione **ALERTAS** > **atual**. "Ver alertas atuais"	Selecione **SUPPORT** > **Alarmes (legacy)** > **Current Alarmes**. "Gerenciar alarmes (sistema legado)"
O que faz com que um alerta ou um alarme seja acionado?	Os alertas são acionados quando uma expressão Prometheus em uma regra de alerta é avaliada como verdadeira para a condição e duração específicas do gatilho. "Ver regras de alerta"	Os alarmes são acionados quando um atributo StorageGRID atinge um valor limite. "Gerenciar alarmes (sistema legado)"
Se um alerta ou alarme for acionado, como resolvo o problema subjacente?	As ações recomendadas para um alerta estão incluídas nas notificações por e-mail e estão disponíveis nas páginas Alertas no Gerenciador de Grade. Conforme necessário, informações adicionais são fornecidas na documentação do StorageGRID. "Referência de alertas"	Você pode aprender sobre um alarme selecionando o nome do atributo ou pode procurar um código de alarme na documentação do StorageGRID. "Referência de alarmes (sistema legado)"
Onde posso ver uma lista de alertas ou alarmes que foram resolvidos?	Selecione **ALERTAS** > **resolvido**. "Ver alertas atuais e resolvidos"	Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes históricos**. "Gerenciar alarmes (sistema legado)"
Onde posso gerir as definições?	Selecione **ALERTAS** > **regras**. "Gerenciar alertas"	Selecione **SUPPORT**. Em seguida, use as opções na seção **Alarmes (legacy)** do menu. "Gerenciar alarmes (sistema legado)"

	Alertas	Alarmes (sistema legado)
Quais permissões do grupo de usuários eu preciso?	• Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alertas atuais e resolvidos. • Você deve ter a permissão Gerenciar alertas para gerenciar silêncios, notificações de alerta e regras de alerta. "Administrar o StorageGRID"	• Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alarmes legados. • Você deve ter a permissão de reconhecer alarmes para reconhecer alarmes. • Você deve ter a configuração da página de topologia de Grade e outras permissões de configuração de grade para gerenciar alarmes globais e notificações de e-mail. "Administrar o StorageGRID"
Como faço para gerenciar notificações por e-mail?	Selecione **ALERTAS** > **Configuração do e-mail**. **Nota:** como os alarmes e alertas são sistemas independentes, a configuração de e-mail usada para notificações de alarme e AutoSupport não é usada para notificações de alerta. No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações. "Configurar notificações por e-mail para alertas"	Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**. "Gerenciar alarmes (sistema legado)"
Como faço para gerenciar notificações SNMP?	Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**. "Utilize a monitorização SNMP"	*Não suportado*
Como posso controlar quem recebe notificações?	1. Selecione **ALERTAS** > **Configuração do e-mail**. 2. 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. "Configurar notificações por e-mail para alertas"	1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**. 2. Criando uma lista de discussão. 3. Selecione **notificações**. 4. Selecione a lista de discussão. "Gerenciar alarmes (sistema legado)"

	Alertas	Alarmes (sistema legado)
Quais nós de administrador enviam notificações?	Um único nó de administração (o remetente preferido). "O que é um nó de administração?"	Um único nó de administração (o remetente preferido). "O que é um nó de administração?"
Como faço para suprimir algumas notificações?	1. Selecione **ALERTAS** > **silêncios**. 2. Selecione a regra de alerta que deseja silenciar. 3. Especifique uma duração para o silêncio. 4. Selecione a gravidade do alerta que deseja silenciar. 5. Selecione para aplicar o silêncio a toda a grade, a um único local ou a um único nó. **Nota**: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam. "Silenciar notificações de alerta"	1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**. 2. Selecione **notificações**. 3. Selecione uma lista de discussão e selecione **suprimir**. "Gerenciar alarmes (sistema legado)"
Como faço para suprimir todas as notificações?	Selecione **ALERTAS** > **silêncios**.em seguida, selecione **todas as regras**. **Nota**: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam. "Silenciar notificações de alerta"	*Não suportado*
Como posso personalizar as condições e os gatilhos?	1. Selecione **ALERTAS** > **regras**. 2. Selecione uma regra padrão para editar ou selecione **criar regra personalizada**. "Editar regras de alerta" "Crie regras de alerta personalizadas"	1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**. 2. Crie um alarme personalizado global para substituir um alarme padrão ou para monitorar um atributo que não tenha um alarme padrão. "Gerenciar alarmes (sistema legado)"

	Alertas	Alarmes (sistema legado)
Como posso desativar um alerta individual ou um alarme?	1. Selecione **ALERTAS** > **regras**. 2. Selecione a regra e selecione **Editar regra**. 3. Desmarque a caixa de seleção **Enabled**. "Desativar regras de alerta"	1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**. 2. Selecione a regra e selecione o ícone Editar. 3. Desmarque a caixa de seleção **Enabled**. "Gerenciar alarmes (sistema legado)"

Gerenciar alertas

Gerenciar alertas: Visão geral

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

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

Para saber mais:

- Reveja o vídeo: "Vídeo: Visão geral dos alertas para o StorageGRID 11,8"
- Reveja o vídeo: "Vídeo: Usando métricas para criar alertas personalizados no StorageGRID 11,8"
- Consulte "Referência de alertas".

Ver regras de alerta

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

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

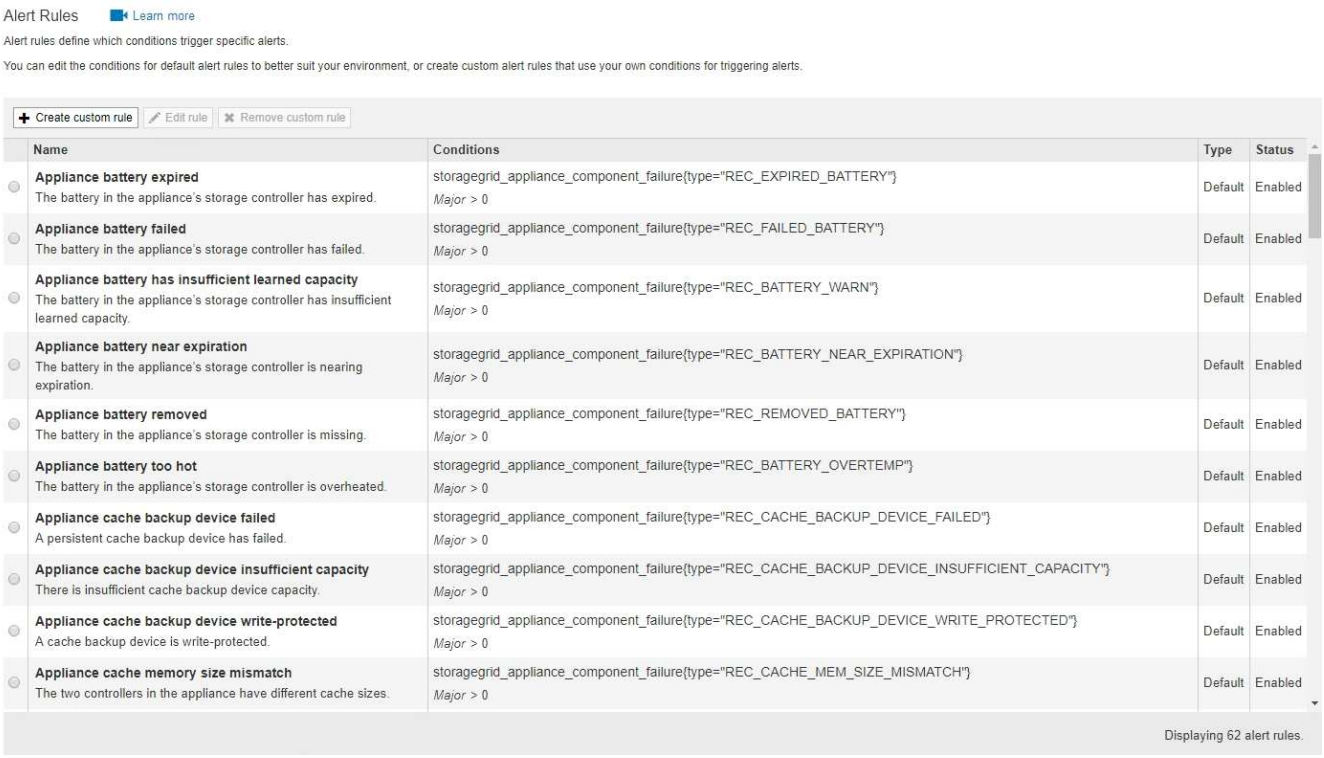
Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".
- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral dos alertas para o StorageGRID 11,8"

Passos

1. Selecione **ALERTAS** > **regras**.

A página regras de alerta é exibida.



2. Reveja 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 Prometheus que determinam quando esse alerta é acionado. Um alerta pode ser acionado 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 StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. • **Major**: 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 pare a operação normal de um nó ou serviço StorageGRID. • **Minor**: o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.

Cabeçalho da coluna	Descrição
Tipo	O tipo de regra de alerta: • **Default**: Uma regra de alerta fornecida com o sistema. Você pode desativar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Não é possível remover uma regra de alerta padrão. • **Padrão***: Uma regra de alerta padrão que inclui uma condição ou duração editada. Conforme necessário, você pode reverter facilmente uma condição modificada de volta ao padrão original. • **Custom**: Uma regra de alerta que você criou. Você pode desativar, editar e remover regras de alerta personalizadas.
Estado	Se esta regra de alerta está atualmente ativada ou desativada. As condições para regras de alerta desativadas 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".
- Você está familiarizado com o "Métricas de Prometheus comumente usadas".
- Você entende o "Sintaxe das consultas Prometheus".
- Opcionalmente, você assistiu o vídeo: "Vídeo: Usando métricas para criar alertas personalizados no StorageGRID 11,8".

Sobre esta tarefa

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

- Observe as condições para as 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 para erros de digitação e lógica.
- Use apenas as métricas listadas na API de Gerenciamento de Grade.
- Ao testar uma expressão usando a API Grid Management, esteja ciente de que uma resposta "bem-sucedida" pode ser um corpo de resposta vazio (nenhum alerta acionado). Para ver se o alerta é realmente acionado, você pode definir temporariamente um limite para um valor que você espera ser verdadeiro atualmente.

Por exemplo, para testar a expressão `node_memory_MemTotal_bytes < 24000000000`, execute primeiro `node_memory_MemTotal_bytes >= 0` e certifique-se de obter 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 essa expressão.

- Não assuma que um alerta personalizado está funcionando, a menos que você tenha validado que o alerta é acionado quando esperado.

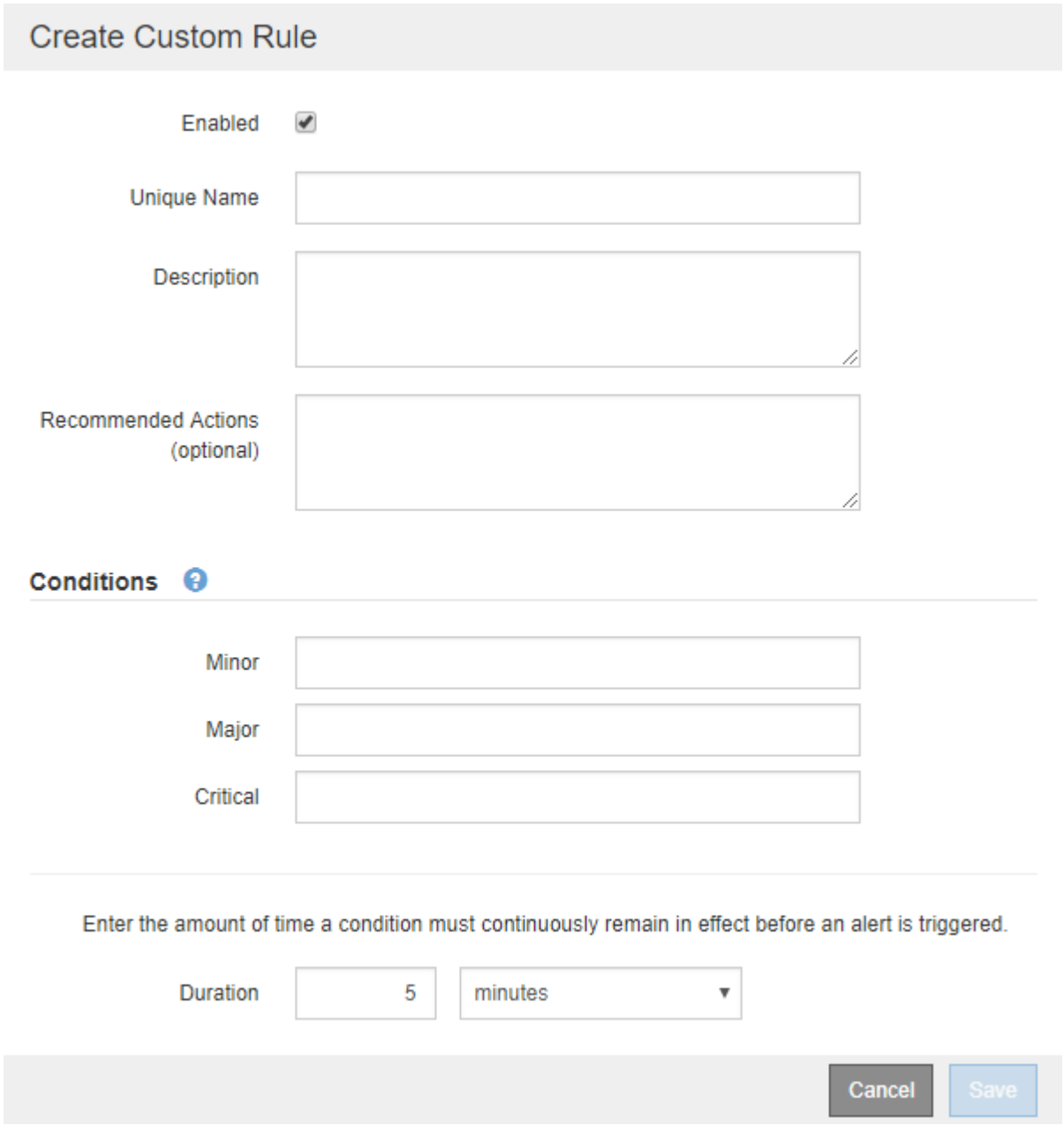
Passos

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 **Enabled** para determinar se essa regra de alerta está ativada no momento.

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

4. Introduza as seguintes informações:

Campo	Descrição
Nome único	Um nome exclusivo para esta regra. O nome da regra de alerta é mostrado 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 carateres.
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta mostrada na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 carateres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando esse 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 carateres.

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

   Uma expressão básica é geralmente da 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 acionado se a quantidade de RAM instalada para um nó for inferior a 24.000.000.000 bytes (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Para ver as métricas disponíveis e testar expressões 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 período de tempo em que uma condição deve permanecer em vigor continuamente 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 **Guardar**.

   A caixa de diálogo fecha-se e a nova regra de alerta personalizada aparece na tabela regras de alerta.

Você pode editar uma regra de alerta para alterar as condições do gatilho. 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Sobre esta tarefa

Ao editar uma regra de alerta padrão, você pode alterar as condições para alertas menores, maiores 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 detete um problema subjacente até que ele impeça que uma operação crítica seja concluída.

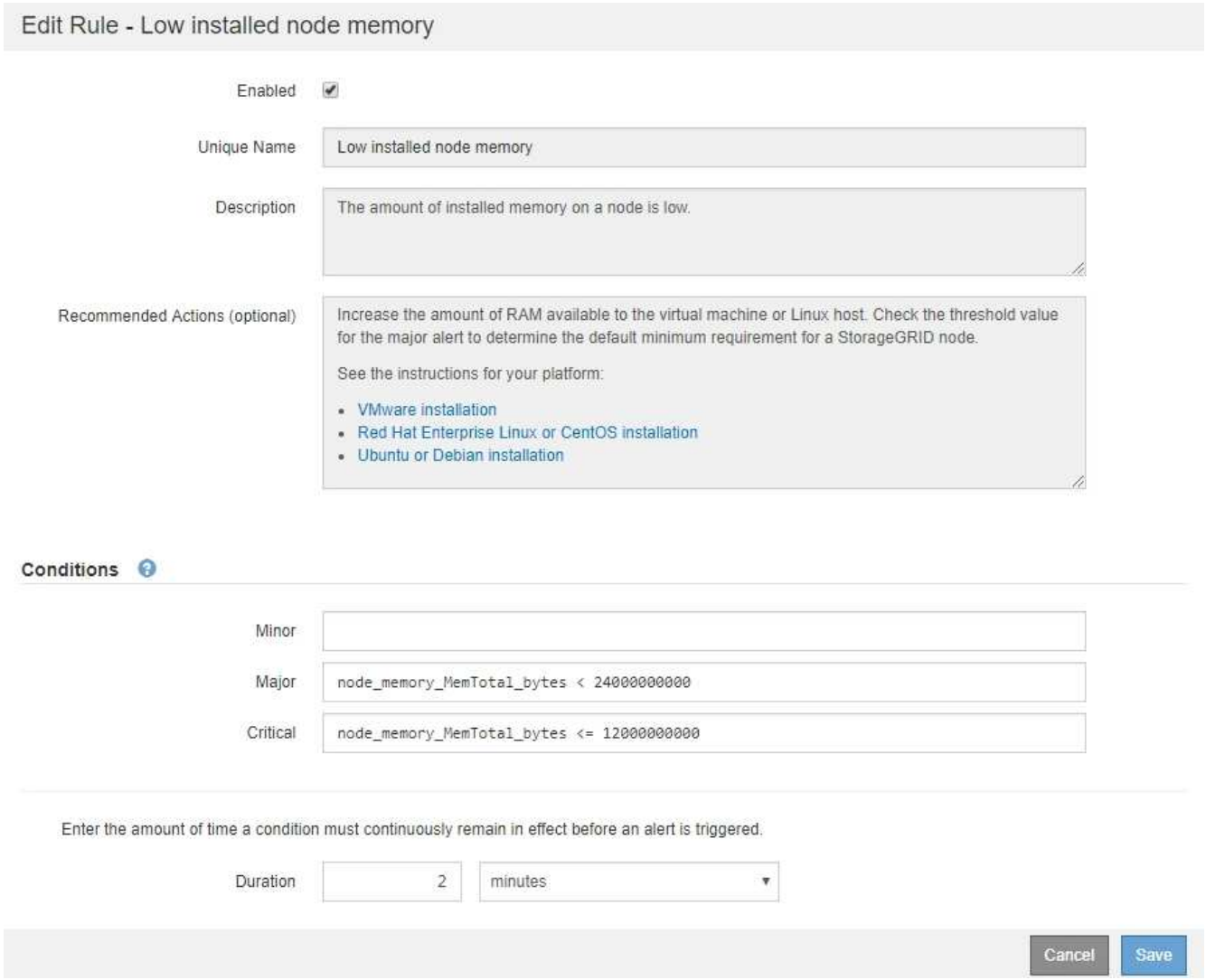
Passos

1. Selecione **ALERTAS** > **regras**.

   A página regras de alerta é exibida.

2. Selecione o botão de opção para a regra de alerta que 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 desativados e não podem ser editados.



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

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

   Se desativar a regra de alerta para um alerta atual, tem de aguardar alguns minutos para que o alerta deixe de aparecer como um alerta ativo.

   Em geral, desativar uma regra de alerta padrão não é recomendado. Se uma regra de alerta estiver desativada, talvez você não detete um problema subjacente até que ela impeça que uma operação crítica seja concluída.

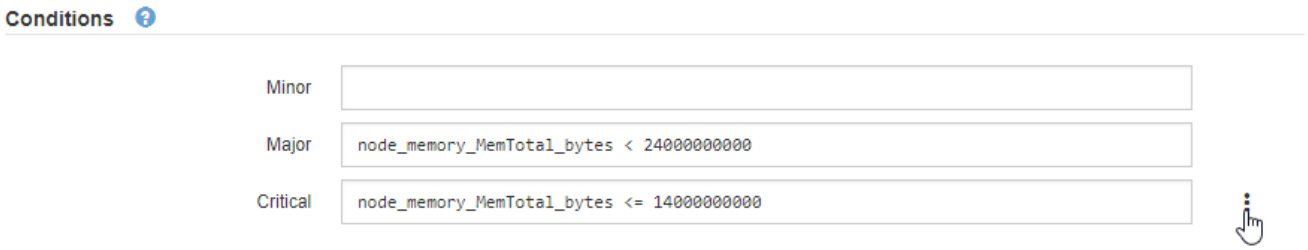
5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.

   Não é possível 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 mostrado 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 carateres.
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta mostrada na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 carateres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando esse 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 carateres.

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

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



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

   Uma expressão básica é geralmente da 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 acionado se a quantidade de RAM instalada para um nó for inferior a 24.000.000.000 bytes (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

7. No campo **duração**, insira o período de tempo em que uma condição deve permanecer em vigor continuamente 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 **Guardar**.

   Se você editou uma regra de alerta padrão, **padrão*** aparecerá na coluna tipo. Se você desativou uma regra de alerta padrão ou personalizada, **Disabled** será exibido na coluna **Status**.

Desativar regras de alerta

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Sobre esta tarefa

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

> Em geral, desativar uma regra de alerta padrão não é recomendado. Se uma regra de alerta estiver desativada, talvez você não detete um problema subjacente até que ela impeça que uma operação crítica seja concluída.

Passos

1. Selecione **ALERTAS** > **regras**.

   A página regras de alerta é exibida.

2. Selecione o botão de opção para a regra de alerta que deseja desativar ou ativar.
3. Selecione **Editar regra**.

   A caixa de diálogo Editar regra é exibida.

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

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

   > Se desativar a regra de alerta para um alerta atual, tem de aguardar alguns minutos para que o alerta deixe de ser apresentado como um alerta ativo.

5. Selecione **Guardar**.

   Disabled 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Passos

1. Selecione **ALERTAS** > **regras**.

   A página regras de alerta é exibida.

2. Selecione o botão de opção para a regra de alerta personalizada que deseja remover.

   Não é possível remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

   É apresentada uma caixa de diálogo de confirmação.

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

   Todas as instâncias ativas do alerta serão resolvidas dentro de 10 minutos.

Gerenciar notificações de alerta

Configurar notificações SNMP para alertas

Se você quiser que o StorageGRID envie notificações SNMP quando ocorrerem alertas, você deverá ativar o agente SNMP do StorageGRID e configurar um ou mais destinos de intercetação.

Você pode usar a opção **CONFIGURATION** > **Monitoring** > **SNMP Agent** no Gerenciador de Grade ou os endpoints SNMP da API de Gerenciamento de Grade para habilitar e configurar o agente SNMP do StorageGRID. O agente SNMP suporta todas as três versões do protocolo SNMP.

Para saber como configurar o agente SNMP, "Utilize a monitorização SNMP"consulte .

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

- Traps são notificações enviadas pelo agente SNMP que não requerem confirmação pelo sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu dentro do StorageGRID, como um alerta sendo acionado. Traps são suportados em todas as três versões do SNMP.
- Os informes são semelhantes aos traps, mas requerem reconhecimento pelo sistema de gestão. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenvia a informação até que uma confirmação seja recebida ou o valor máximo de tentativa tenha sido atingido. As informações são suportadas em SNMPv2c e SNMPv3.

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

Se a sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal é o remetente preferido para notificações de alerta, pacotes AutoSupport, traps e informes SNMP e notificações de alarme herdadas. Se o nó de administração principal ficar indisponível, as notificações serão enviadas

temporariamente por outros nós de administração. "O que é um nó de administração?"Consulte .

Configurar notificações por e-mail para alertas

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Sobre esta tarefa

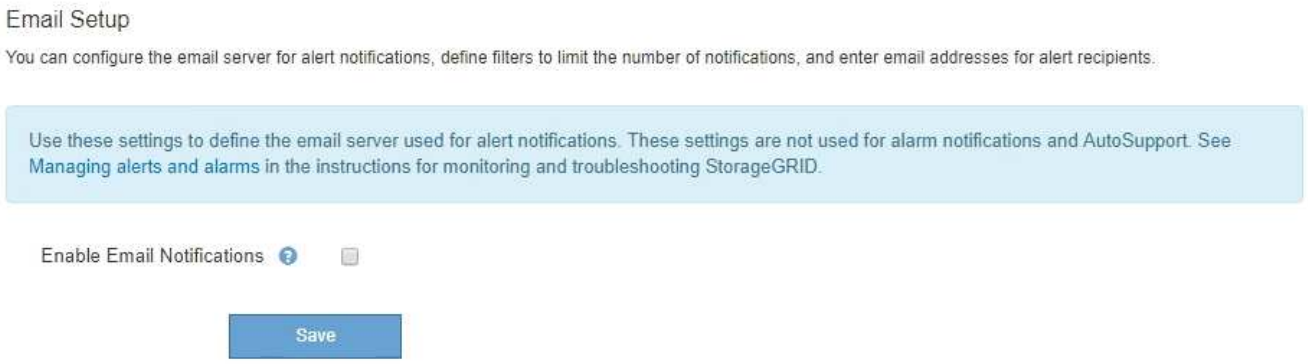
Como os alarmes e alertas são sistemas independentes, a configuração de e-mail usada para notificações de alerta não é usada para notificações de alarme e pacotes AutoSupport. No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações.

Se a sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal é o remetente preferido para notificações de alerta, pacotes AutoSupport, traps e informes SNMP e notificações de alarme herdadas. Se o nó de administração principal ficar indisponível, as notificações serão enviadas temporariamente por outros nós de administração. "O que é um nó de administração?"Consulte .

Passos

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

   A página Configuração de e-mail é exibida.



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

   As seções servidor de e-mail (SMTP), TLS (Transport Layer Security), 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 servidor SMTP exigir autenticação, você deve fornecer um nome de usuário e uma senha.

Campo	Introduza
Servidor de correio	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do servidor SMTP.
Porta	A porta usada para acessar o servidor SMTP. Deve estar entre 1 e 65535.
Nome de utilizador (opcional)	Se o servidor SMTP exigir autenticação, insira o nome de usuário com o qual se autenticar.
Senha (opcional)	Se o servidor SMTP exigir autenticação, introduza a palavra-passe com a qual pretende autenticar.

4. Na seção endereços de e-mail, insira endereços de e-mail para o remetente e para cada destinatário.

   a. Para **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 TLS (Transport Layer Security) for necessária para comunicações com o servidor SMTP, selecione **Require TLS** na seção TLS (Transport Layer Security).

   a. No campo **certificado CA**, forneça o certificado CA que será usado para verificar a identificação 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 de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

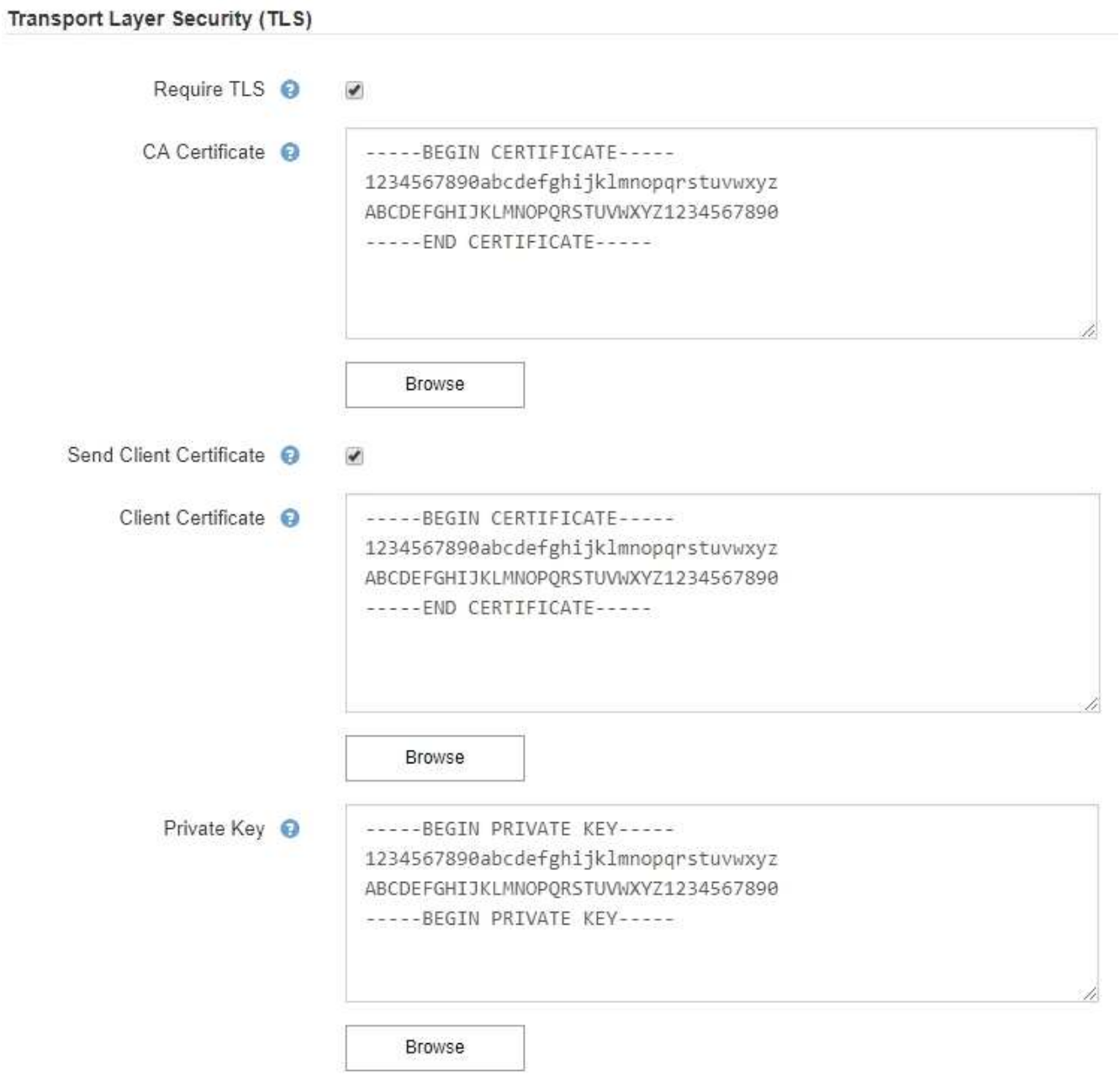
b. Marque a caixa de seleção **Send Client Certificate** se o servidor de e-mail SMTP exigir que os remetentes de e-mail forneçam certificados de cliente para autenticação.
c. No campo **Client Certificate**, forneça o certificado de cliente codificado em PEM para enviar para o servidor SMTP.

   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 for necessário 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 de 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 de uma regra de alerta é atendida. As notificações não são enviadas para alertas menores.

Gravidade	Descrição
Apenas crítica	Uma notificação por e-mail é enviada somente quando a condição crítica de uma regra de alerta é atendida. As 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. Marque 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 poucos minutos ou se o alerta **Falha na notificação por e-mail** for acionado, verifique as configurações e tente novamente.

   c. Faça login em qualquer outro nó Admin e envie um e-mail de teste para verificar a conetividade de todos os sites.

      Ao testar notificações de alerta, você deve entrar em cada nó de administração para verificar a conetividade. Isso é em contraste com o teste de pacotes AutoSupport e notificações de alarme legadas, onde todos os nós de administração enviam o e-mail de teste.

8. Selecione **Guardar**.

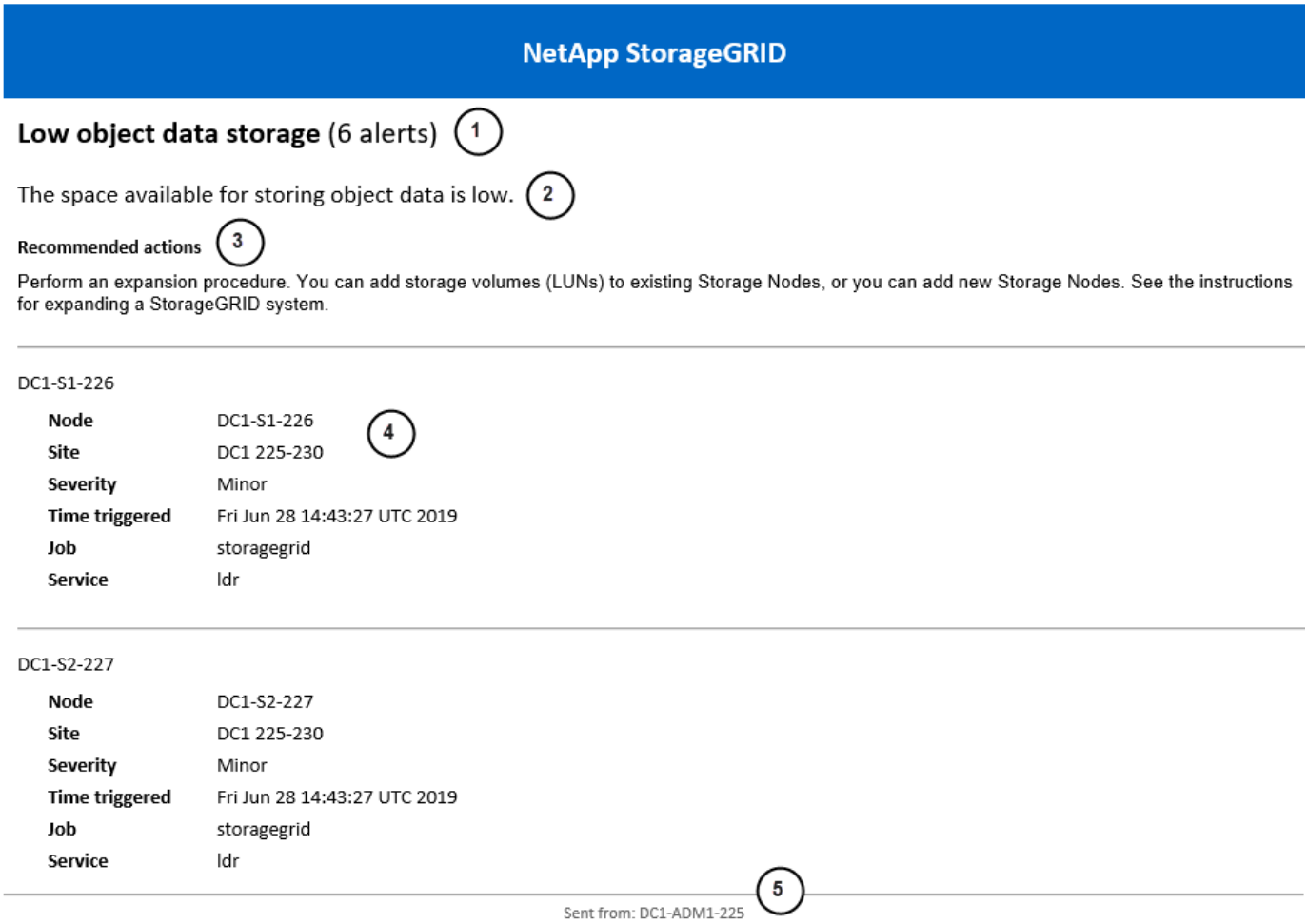
   Enviar um e-mail de teste não salva suas configurações. Você deve selecionar **Salvar**.

   As configurações de e-mail são salvas.

Informações incluídas nas notificações por e-mail de alerta

Depois de configurar o servidor de e-mail SMTP, as notificações de e-mail são enviadas aos destinatários designados quando um alerta é acionado, a menos que a regra de alerta seja suprimida por um silêncio. "Silenciar notificações de alerta"Consulte .

As notificações por e-mail incluem as seguintes informações:



Legenda	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, a hora UTC em que a regra de alerta foi acionada e o nome da tarefa e serviço afetados.
5	O nome do host do nó Admin 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 aplica-se apenas a alertas com o mesmo nome. Se dois alertas com nomes diferentes forem acionados 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 por 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 acionado, o StorageGRID aguarda 2 minutos antes de enviar uma notificação. Se outros alertas com o mesmo nome forem acionados durante esse período, o StorageGRID agrupa 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 um outro alerta com o mesmo nome for acionado, o StorageGRID aguarda 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 reportados 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 desses alertas 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 foi 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 a enviar 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 ou silenciado. Notificações adicionais são enviadas em 15 de março, 22 de março, 29 de março, e assim por diante.

Solucionar problemas de notificações por e-mail de alerta

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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Passos

1. Verifique as suas definições.
   a. Selecione **ALERTAS** > **Configuração do 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 o filtro de spam e certifique-se de que o e-mail não foi enviado para uma pasta de lixo eletrônico.
3. Peça ao administrador de e-mail para confirmar que os e-mails do endereço do remetente não estão sendo bloqueados.
4. Colete um arquivo de log para o Admin Node 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 se conetar ao servidor especificado.

   "Colete arquivos de log e dados do sistema"Consulte .

Silenciar notificações de alerta

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Gerencie alertas ou permissão de acesso root".

Sobre esta tarefa

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

Se tiver ativado o agente SNMP, os silêncios também suprimem traps SNMP e informam.

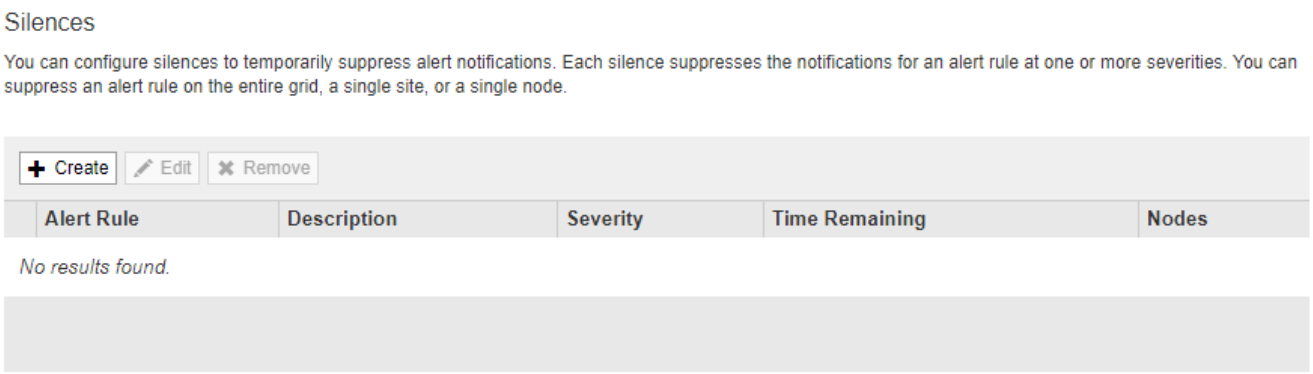
> Tenha cuidado ao decidir silenciar uma regra de alerta. Se você silenciar um alerta, talvez não detete um problema subjacente até que ele impeça que uma operação crítica seja concluída.

> Como os alarmes e alertas são sistemas independentes, você não pode usar essa funcionalidade para suprimir as notificações de alarme.

Passos

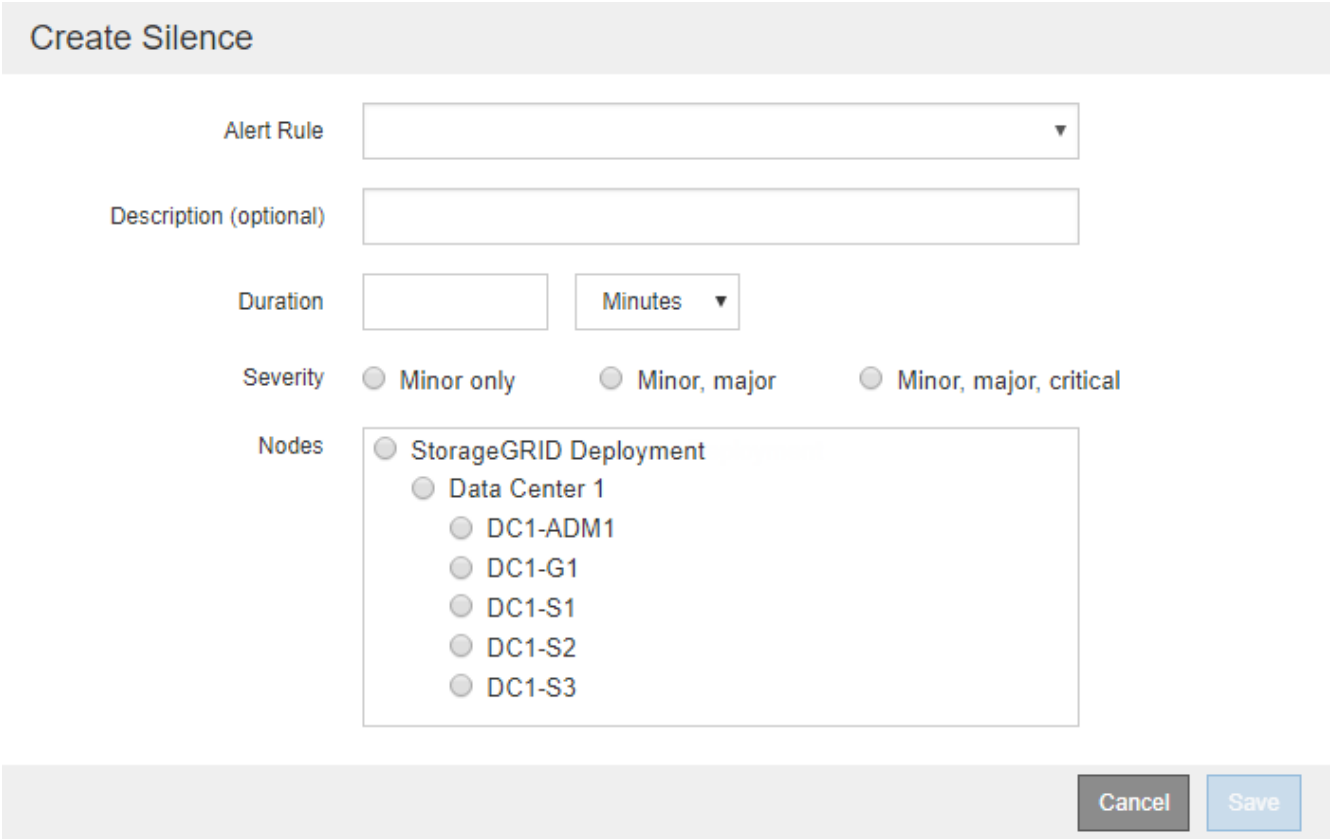
1. Selecione **ALERTAS** > **silêncios**.

   É apresentada a página silêncios.



2. Selecione **criar**.

   A caixa de diálogo criar Silêncio é exibida.



3. Selecione ou introduza 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 desativada. **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 deste silêncio.
Duração	Quanto tempo você quer que esse silêncio permaneça em vigor, em minutos, horas ou dias. Um silêncio pode estar em vigor de 5 minutos a 1.825 dias (5 anos). **Nota:** você não deve silenciar uma regra de alerta por um período prolongado de tempo. Se uma regra de alerta for silenciada, talvez você não detete um problema subjacente até que ela impeça que uma operação crítica seja concluída. No entanto, talvez seja necessário usar um silêncio prolongado se um alerta for acionado por uma configuração específica e intencional, como pode ser o caso dos alertas de link do **Services Appliance para baixo** e dos alertas de link do Storage Appliance para baixo*.
Gravidade	Que gravidade de alerta ou severidades devem ser silenciadas. Se o alerta for acionado em uma das severidades selecionadas, nenhuma notificação será enviada.
Nós	A que nó ou nós você deseja que esse silêncio se aplique. Você pode suprimir uma regra de alerta ou todas as regras em toda a grade, em um único local ou em um único nó. Se selecionar toda a grelha, o silêncio aplica-se a todos os locais e a todos os nós. Se selecionar um local, o silêncio aplica-se apenas aos nós nesse local. **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 local de cada vez.

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

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

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

Informações relacionadas

- "Configure o agente SNMP"

Referência de alertas

Esta referência lista os alertas padrão que aparecem no Gerenciador de Grade. 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 Prometheus"o .

Alertas de dispositivo

Nome do alerta	Descrição
A bateria do aparelho expirou	A bateria do controlador de armazenamento do aparelho expirou.
A bateria do aparelho falhou	A bateria do controlador de armazenamento do aparelho falhou.
A bateria do aparelho não tem capacidade programada suficiente	A bateria do controlador de armazenamento do aparelho não tem capacidade de aprendizagem suficiente.
A bateria do aparelho está quase a expirar	A bateria do controlador de armazenamento do aparelho está prestes a expirar.
Bateria do aparelho removida	A bateria do controlador de armazenamento do aparelho está em falta.
Bateria do aparelho demasiado quente	A bateria do controlador de armazenamento do aparelho está sobreaquecida.
Erro de comunicação do Appliance BMC	A comunicação com o controlador de gestão do rodapé (BMC) foi perdida.

Nome do alerta	Descrição
Falha no dispositivo de backup do cache do dispositivo	Um dispositivo de backup de cache persistente falhou.
Dispositivo de backup de cache de dispositivo capacidade insuficiente	Não há capacidade insuficiente do dispositivo de backup em cache.
Dispositivo de backup protegido contra gravação em cache do dispositivo	Um dispositivo de backup em cache está protegido contra gravação.
Incompatibilidade do tamanho da memória cache do dispositivo	Os dois controladores no dispositivo têm tamanhos de cache diferentes.
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 detetada no controlador de computação de um dispositivo StorageGRID.
A fonte de Alimentação A do controlador de computação do dispositivo tem um problema	A fonte de Alimentação A no controlador de computação tem um problema.
A fonte de alimentação B do controlador de computação do dispositivo tem um problema	A fonte de alimentação B no controlador de computação tem um problema.
O serviço de monitor de hardware de computação do dispositivo parou	O serviço que monitora o status do hardware de storage parou.
A unidade DAS do dispositivo excede o limite para dados gravados por dia	Uma quantidade excessiva de dados está sendo gravada em uma unidade todos os dias, o que pode anular sua garantia.
Detectada avaria na unidade DAS do aparelho	Foi detetado um problema com uma unidade de armazenamento de ligação direta (DAS) no aparelho.
Luz de localização da unidade do aparelho DAS acesa	A luz do localizador de unidades para uma ou mais unidades de armazenamento de conexão direta (DAS) em um nó de armazenamento de dispositivos está acesa.

Nome do alerta	Descrição
Reconstrução da unidade DAS do dispositivo	Uma unidade de armazenamento de conexão direta (DAS) está sendo reconstruída. Isto é esperado se tiver sido recentemente substituído ou removido/reinserido.
Detetada avaria na ventoinha do aparelho	Foi detetado um problema com uma ventoinha no aparelho.
Detectada avaria no canal de fibra do dispositivo	Foi detetado um problema de link Fibre Channel entre o controlador de storage do dispositivo e o controlador de computação
Falha na porta HBA Fibre Channel do dispositivo	Uma porta HBA Fibre Channel está falhando ou falhou.
O cache flash do dispositivo não é ideal	As unidades usadas para o cache SSD não são ideais.
Recipiente da bateria/interligação do aparelho removido	O depósito da bateria/interligação está em falta.
Porta LACP do aparelho em falta	Uma porta em um dispositivo StorageGRID não está participando da ligação LACP.
Detectada falha na NIC do aparelho	Foi detetado um problema com uma placa de interface de rede (NIC) no dispositivo.
A fonte de alimentação geral do aparelho está degradada	A alimentação de um aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.
Aviso crítico de SSD do dispositivo	Um SSD de dispositivo está relatando um aviso crítico.
Falha do controlador de storage do dispositivo A	O controlador de storage A em um dispositivo StorageGRID falhou.
Falha no controlador B de storage do dispositivo	O controlador de storage B em um dispositivo StorageGRID falhou.
Falha na unidade do controlador de armazenamento do dispositivo	Uma ou mais unidades em um dispositivo StorageGRID falhou ou não é ideal.
Problema de hardware do controlador de storage do dispositivo	O software SANtricity está relatando "precisa de atenção" para um componente em um dispositivo StorageGRID.
Falha na fonte de alimentação do controlador de armazenamento do dispositivo	A fonte de Alimentação A num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.

Nome do alerta	Descrição
Falha na fonte de alimentação B do controlador de armazenamento do dispositivo	A fonte de alimentação B num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.
O serviço de monitor de hardware de armazenamento do dispositivo parou	O serviço que monitora o status do hardware de storage parou.
Prateleiras de storage do dispositivo degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento é degradado.
Temperatura do aparelho excedida	A temperatura nominal ou máxima para o 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 appliance	Um aparelho não foi inicializado com segurança.
A e/S do disco é muito lenta	E/S de disco muito lento pode estar impactando o desempenho da grade.
Detectada avaria na ventoinha do aparelho de armazenamento	Foi detetado um problema com um ventilador no controlador de armazenamento de um aparelho.
Conectividade de storage do dispositivo de storage degradada	Há um problema com uma ou mais conexões entre o controlador de computação e o controlador de storage.
Dispositivo de armazenamento inacessível	Não é possível aceder a 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 sendo preenchida.
Erro de encaminhamento do servidor syslog externo	O nó não pode encaminhar logs para o servidor syslog externo.
Fila de auditoria grande	A fila de discos para mensagens de auditoria está cheia. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.

Nome do alerta	Descrição
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 sendo preenchida.

Alertas de intervalo

Nome do alerta	Descrição
O balde FabricPool tem uma definição de consistência do balde não suportada	Um bucket do FabricPool usa o nível de consistência disponível ou de sites fortes, que não é suportado.

Alertas do Cassandra

Nome do alerta	Descrição
Erro de auto-compactador Cassandra	O auto-compactador Cassandra sofreu um erro.
Métricas do compactador automático Cassandra desatualizadas	As métricas que descrevem o compactador automático Cassandra estão desatualizadas.
Erro de comunicação Cassandra	Os nós que executam o serviço Cassandra estão tendo problemas para se comunicar uns com os outros.
Cassandra compactions sobrecarregado	O processo de compactação Cassandra está sobrecarregado.
Erro de gravação de tamanho excessivo do Cassandra	Um processo interno do StorageGRID enviou uma solicitação de gravação para o Cassandra que era muito grande.
Métricas de reparo do Cassandra desatualizadas	As métricas que descrevem os trabalhos de reparo do Cassandra estão desatualizadas.
O progresso do reparo do Cassandra lento	O progresso dos reparos do banco de dados Cassandra é lento.
O serviço de reparação Cassandra não está disponível	O serviço de reparação Cassandra não está disponível.
Corrupção da tabela Cassandra	Cassandra detetou corrupção de tabela. O Cassandra reinicia automaticamente se detetar corrupção de tabela.

Alertas do Cloud Storage Pool

Nome do alerta	Descrição
Erro de conetividade do Cloud Storage Pool	A verificação de integridade dos pools de armazenamento em nuvem detetou um ou mais erros novos.

Alertas de replicação entre grades

Nome do alerta	Descrição
Falha permanente de replicação entre redes	Ocorreu um erro de replicação entre redes que requer a intervenção do utilizador para resolver.
Recursos de replicação entre grades indisponíveis	As solicitações de replicação entre grade estão pendentes porque um recurso não está disponível.

Alertas DHCP

Nome do alerta	Descrição
A concessão DHCP expirou	A concessão de DHCP numa interface de rede expirou.
A concessão DHCP expira em breve	A concessão de DHCP em uma interface de rede está expirando em breve.
Servidor DHCP indisponível	O servidor DHCP não está disponível.

Depurar e rastrear alertas

Nome do alerta	Descrição
Impacto no desempenho de depuração	Quando o modo de depuração está ativado, o desempenho do sistema pode ser afetado negativamente.
Configuração do traçado ativada	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 AutoSupport	Não foi possível enviar a mensagem AutoSupport mais recente.
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail para um alerta.

Alertas de codificação de apagamento (EC)

Nome do alerta	Descrição
Falha no rebalanceamento EC	O procedimento de reequilíbrio CE falhou ou foi interrompido.
Falha na reparação EC	Um trabalho de reparação para dados EC falhou ou foi interrompido.
A reparação CE parou	Um trabalho de reparação para dados CE parou.

Expiração de alertas de certificados

Nome do alerta	Descrição
Expiração do certificado CA do Proxy Admin	Um ou mais certificados no pacote de CA do servidor proxy administrativo está prestes a expirar.
Expiração do certificado do cliente	Um ou mais certificados de cliente estão prestes a expirar.
Expiração do certificado de servidor global para S3 e Swift	O certificado de servidor global para S3 e Swift está prestes a expirar.
Expiração do certificado de ponto final do balanceador de carga	Um ou mais certificados de endpoint do balanceador de carga estão prestes a expirar.
Expiração do certificado do servidor para a 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 de autoridade de certificação (CA) usado para assinar o certificado de servidor syslog externo está prestes a expirar.
Expiração do certificado do cliente syslog externo	O certificado de cliente para um servidor syslog externo está prestes a expirar.
Expiração do certificado do servidor syslog externo	O certificado de servidor apresentado pelo servidor syslog externo está prestes a expirar.

Alertas da rede de grelha

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

Alertas de federação de grade

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

Alertas de alta utilização ou alta latência

Nome do alerta	Descrição
Alto uso de heap Java	Uma alta porcentagem de espaço de heap 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 origem da identidade.
Falha na sincronização da federação de identidade para um locatário	Não é possível sincronizar grupos federados e usuários da origem de identidade configurada por um locatário.

Alertas de gerenciamento do ciclo de vida das informações (ILM)

Nome do alerta	Descrição
Colocação de ILM inalcançável	Uma instrução de colocação em uma regra ILM não pode ser alcançada para determinados objetos.
Período de digitalização ILM demasiado longo	O tempo necessário para digitalizar, avaliar e aplicar ILM a objetos é muito longo.
Taxa de digitalização ILM baixa	A taxa de digitalização ILM é definida para menos de 100 objetos/segundo.

Alertas de servidor de gerenciamento de chaves (KMS)

Nome do alerta	Descrição
Expiração do certificado CA de KMS	O certificado de autoridade de certificação (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.

Nome do alerta	Descrição
Expiração do certificado do cliente KMS	O certificado de cliente para um servidor de gerenciamento de chaves está prestes a expirar
Falha ao carregar a configuração DE KMS	A configuração para o servidor de gerenciamento de chaves existe, mas não foi possível carregar.
Erro de conetividade DE KMS	Um nó de dispositivo não pôde se conetar ao servidor de gerenciamento de chaves para seu site.
Nome da chave de encriptação 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 KMS	Todos os volumes de dispositivos foram descriptografados com êxito, mas um ou mais volumes não puderam girar para a chave mais recente.
KMS não está configurado	Não existe nenhum servidor de gerenciamento de chaves para este site.
A chave KMS falhou ao desencriptar um volume de aparelho	Um ou mais volumes em um dispositivo com criptografia de nó ativada não puderam ser descriptografados com a chave KMS atual.
Expiração do certificado do servidor DE KMS	O certificado do servidor usado pelo KMS (Key Management Server) está prestes a expirar.

Alertas de desvio do relógio local

Nome do alerta	Descrição
Desvio de tempo grande do relógio local	O desvio entre o relógio local e a hora do NTP (Network Time Protocol) é demasiado grande.

Alertas de memória baixa ou de espaço reduzido

Nome do alerta	Descrição
Baixa capacidade de disco de log de auditoria	O espaço disponível para logs de auditoria é baixo. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Baixa memória disponível do nó	A quantidade de RAM disponível em um nó é baixa.
Baixo espaço livre para piscina de armazenamento	O espaço disponível para armazenar dados de objetos no nó de armazenamento é baixo.
Baixa memória do nó instalada	A quantidade de memória instalada em um nó é baixa.

Nome do alerta	Descrição
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.
Baixo armazenamento de dados de objetos	O espaço disponível para armazenar dados de objetos é baixo.
Baixa sobreposição de marca d'água somente leitura	A Sobreposição da marca d'água apenas de leitura suave do volume de armazenamento é inferior à marca d'água mínima otimizada para um nó de armazenamento.
Baixa capacidade de 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 esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Espaço livre do diretório de baixa tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de rede de nós ou nós

Nome do alerta	Descrição
Admin Network receber uso	O uso de receção na rede Admin é alto.
Utilização de transmissão de rede Admin	A utilização de transmissão na rede de administração é elevada.
Falha na configuração do firewall	Falha ao aplicar a configuração da firewall.
Endpoints de interface de gerenciamento no modo fallback	Todos os endpoints de interface de gerenciamento têm voltado para as portas padrão por muito tempo.
Erro de conetividade de rede do nó	Ocorreram erros durante a transferência de dados entre nós.
Erro de quadro de receção de rede do nó	Uma alta porcentagem dos quadros de rede recebidos por um nó teve erros.
Nó não sincronizado com o servidor NTP	O nó não está em sincronia com o servidor NTP (Network Time Protocol).
Nó não bloqueado com servidor NTP	O nó não está bloqueado para um servidor NTP (Network Time Protocol).

Nome do alerta	Descrição
Rede de nós que não são do dispositivo inativa	Um ou mais dispositivos de rede estão inativos ou desconetados.
Link do utilitário de serviços para baixo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do utilitário de serviços para baixo na porta de rede Admin 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.
Link do utilitário de serviços para baixo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.
Link do dispositivo de armazenamento na rede Admin	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do dispositivo de armazenamento na porta Admin Network 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.
Ligação do dispositivo de armazenamento na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.

Nome do alerta	Descrição
Nó de storage não no estado de storage 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
Utilização da ligação 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 reinicializou inesperadamente nas últimas 24 horas.

Alertas de objetos

Nome do alerta	Descrição
Falha na verificação de existência do objeto	O trabalho de verificação de existência de objeto falhou.
Verificação de existência de objeto parada	O trabalho de verificação de existência de objeto parou.
Objetos perdidos	Um ou mais objetos foram perdidos da grade.
S3 COLOQUE o tamanho do objeto muito grande	Um cliente está tentando uma operação PUT Object que excede os limites de tamanho S3.
Objeto corrompido não identificado detetado	Um arquivo foi encontrado no storage de objetos replicado que não pôde ser identificado como um objeto replicado.

Alertas de serviços de plataforma

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

Alertas de volume de storage

Nome do alerta	Descrição
O volume de armazenamento precisa de atenção	Um volume de armazenamento está offline e precisa de atenção.
O volume de storage precisa ser restaurado	Um volume de armazenamento foi recuperado e precisa ser restaurado.
Volume de armazenamento offline	Um volume de armazenamento está offline por mais de 5 minutos, possivelmente porque o nó reinicializou durante a etapa de formatação do volume.
Falha ao iniciar o reparo de dados replicados	O reparo de dados replicados para um volume reparado não pôde ser iniciado automaticamente.

Alertas dos serviços do StorageGRID

Nome do alerta	Descrição
serviço nginx usando configuração de backup	A configuração do serviço nginx é inválida. A configuração anterior está agora a ser utilizada.
serviço nginx-gw usando configuração de backup	A configuração do serviço nginx-gw é inválida. A configuração anterior está agora a ser utilizada.
É necessário reiniciar para desativar o FIPS	A diretiva de segurança não requer o modo FIPS, mas o módulo de segurança criptográfico NetApp está ativado.
É necessário reiniciar para ativar o FIPS	A diretiva de segurança requer o modo FIPS, mas o módulo de segurança criptográfico NetApp está desativado.
Serviço SSH usando configuração de backup	A configuração do serviço SSH é inválida. A configuração anterior está agora a ser utilizada.

Alertas do locatário

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

Métricas de 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 obtenha uma lista completa de todas as métricaspode .

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

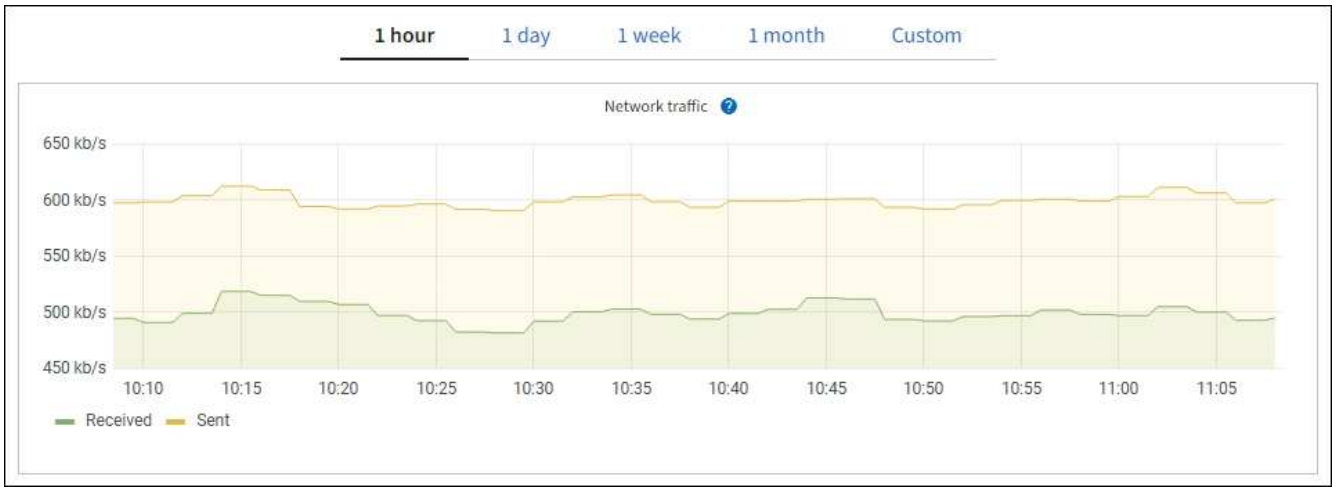
O que são métricas Prometheus?

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

Onde são usadas as métricas do Prometheus?

As métricas coletadas por Prometheus são usadas em vários locais do Grid Manager:

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



- **Alertas**: Os alertas são acionados em níveis específicos de gravidade quando as condições de regra de alerta que usam métricas Prometheus avaliam como verdadeiras.
- * API de gerenciamento de grade*: Você pode usar métricas 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 Grid Management. (Na parte superior do Gerenciador de Grade, 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.

> As 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 **SUPPORT** > **Tools** > **Diagnostics** e a página **SUPPORT** > **Tools** > **Metrics**: Essas páginas, que são destinadas principalmente ao uso por suporte técnico, fornecem várias ferramentas e gráficos que usam os valores das métricas Prometheus.

> Alguns recursos e itens de menu dentro da página Metrics são intencionalmente não funcionais e estão sujeitos a alterações.

Lista das métricas mais comuns

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

> As 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.

node_filesystem_avail_bytes
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.

node_network_carrier
Valor do transportador `/sys/class/net/iface` de .

node_network_receive_errs_total
Estatística do dispositivo de rede `receive_errs` .

node_network_transmit_errs_total
Estatística do dispositivo de rede `transmit_errs` .

StorageGRID_administrativamente_down
O nó não está conetado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado.

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

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

StorageGRID_appliance_storage_controller_hardware_status
O status geral do hardware do controlador de storage em um dispositivo.

StorageGRID_content_buckets_and_containers
O número total de buckets S3 e contentores Swift conhecidos por este nó de armazenamento.

StorageGRID_content_objects
O número total de objetos de dados S3 e Swift conhecido por este nó de storage. A contagem é válida apenas para objetos de dados criados por aplicativos clientes que fazem interface com o sistema através de S3 ou Swift.

StorageGRID_content_objects_lost
O número total de objetos que este serviço deteta 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"

StorageGRID_http_sessions_incoming_tented

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

StorageGRID_http_sessions_incoming_currently_established

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 êxito, seja devido a uma solicitação HTTP mal formada ou a uma falha durante o processamento de uma operação.

StorageGRID_http_sessions_incoming_successful

O número total de sessões HTTP concluídas com êxito.

StorageGRID_ilm_awaiting_background_objects

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

StorageGRID_ilm_awaiting_client_evaluation_objects_per_second

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

StorageGRID_ilm_awaiting_client_objects

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

StorageGRID_ilm_awaiting_total_objects

O número total de objetos aguardando avaliação ILM.

StorageGRID_ilm_scan_objects_per_second

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

StorageGRID_ilm_scan_period_estimated_minutes

O tempo estimado para concluir uma verificação completa do ILM neste nó.

Nota: Uma verificação completa não garante que o ILM tenha sido aplicado a todos os objetos pertencentes a este nó.

StorageGRID_load_balancer_endpoint_cert_expiry_time

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

StorageGRID_metadata_queries_average_latency_milésimos de segundo

O tempo médio necessário para executar uma consulta contra o armazenamento de metadados através deste serviço.

StorageGRID_network_received_bytes

A quantidade total de dados recebidos desde a instalação.

StorageGRID_network_transmitted_bytes

A quantidade total de dados enviados desde a instalação.

StorageGRID_node_cpu_utilization_percentage

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

servidor.

StorageGRID_ntp_chosen_time_source_offset_milissegundos

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

StorageGRID_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

A quantidade total de dados recuperados por clientes S3 a partir deste nó de armazenamento desde que o atributo foi redefinido pela última vez.

storagegrid_s3_operations_failed

O número total de operações S3 falhadas (códigos de status HTTP 4xx e 5xx), excluindo aquelas causadas por falha de autorização do 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 falhadas que resultam de uma falha de autorização.

StorageGRID_servercertificate_management_interface_cert_expiry_days

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 do certificado da API de armazenamento de objetos expirar.

StorageGRID_service_cpu_seconds

O período de tempo acumulado em que a CPU foi utilizada por este serviço desde a instalação.

StorageGRID_service_memory_usage_bytes

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

StorageGRID_service_network_received_bytes

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

StorageGRID_service_network_transmitted_bytes

A quantidade total de dados enviados por este serviço.

StorageGRID_service_restarts

O número total de vezes que o serviço foi reiniciado.

StorageGRID_service_runtime_seconds

O tempo total em que o serviço foi executado desde a instalação.

StorageGRID_service_uptime_seconds

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

StorageGRID_storage_state_current

O estado atual dos serviços de storage. Os valores de atributo são:

- 10: Offline
- 15: Manutenção
- 20 - somente leitura
- 30 - Online

StorageGRID_storage_status

O status atual dos serviços de storage. Os valores de atributo são:

- 0: Sem erros
- 10: Em transição
- 20: Espaço livre insuficiente
- 30 volume(s) indisponível(s)
- 40 - erro

StorageGRID_storage_utilization_data_bytes

Uma estimativa do tamanho total de dados de objetos replicados e codificados por apagamento no nó de storage.

StorageGRID_storage_utilization_metadata_allowed_bytes

O espaço total no volume 0 de cada nó de storage permitido para metadados de objetos. 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 de 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.

StorageGRID_storage_utilization_metadata_bytes

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

StorageGRID_storage_utilization_total_space_bytes

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

StorageGRID_storage_utilization_usable_space_bytes

A quantidade total de espaço de armazenamento de objetos restante. Calculado adicionando a quantidade de espaço disponível para todos os armazenamentos de objetos no nó de armazenamento.

StorageGRID_swift_data_transfers_bytes_ingerido

A quantidade total de dados ingerida de clientes Swift para este nó de armazenamento desde que o atributo foi redefinido pela última vez.

StorageGRID_swift_data_transfers_bytes_recuperados

A quantidade total de dados recuperados pelos clientes Swift deste nó de armazenamento desde que o atributo foi redefinido pela última vez.

StorageGRID_swift_operations_failed

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

StorageGRID_swift_operations_successful

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

StorageGRID_swift_operations_unauthorized

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

StorageGRID_tenant_usage_data_bytes

O tamanho lógico de todos os objetos para o locatário.

StorageGRID_tenant_use_object_count

O número de objetos para o inquilino.

StorageGRID_tenant_usage_quota_bytes

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 Grid Management.

1. Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Localize as operações **metrics**.
3. Execute a `GET /grid/metric-names` operação.
4. Faça o download dos resultados.

Gerenciar alarmes (sistema legado)

Gerenciar alarmes (sistema legado)

O sistema de alarme StorageGRID é o sistema legado usado para identificar pontos de problemas que às vezes ocorrem durante a operação normal.

> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Classes de alarme (sistema legado)

Um alarme legado pode pertencer a uma das duas classes de alarme mutuamente exclusivas.

- Os alarmes padrão são fornecidos com cada sistema StorageGRID e não podem ser modificados. No entanto, você pode desativar os alarmes padrão ou substituí-los definindo alarmes personalizados globais.

- Os alarmes personalizados globais monitoram o status de todos os serviços de um determinado tipo no sistema StorageGRID. Você pode criar um alarme personalizado global para substituir um alarme padrão. Você também pode criar um novo alarme Global Custom. Isso pode ser útil para monitorar quaisquer condições personalizadas do seu sistema StorageGRID.

Lógica de acionamento de alarme (sistema legado)

Um alarme legado é acionado quando um atributo StorageGRID atinge um valor limite que é avaliado como verdadeiro em relação a uma combinação de classe de alarme (padrão ou Personalizado Global) e nível de gravidade de alarme.

Ícone	Cor	Gravidade do alarme	Significado
	Amarelo	Aviso	O nó está conetado à grade, mas existe uma condição incomum que não afeta as operações normais.
	Laranja claro	Menor	O nó está conetado à grade, mas existe uma condição anormal que pode afetar a operação no futuro. Você deve investigar para evitar o escalonamento.
	Laranja escuro	Maior	O nó está conetado à grade, mas existe uma condição anormal que afeta atualmente a operação. Isso requer atenção imediata para evitar o escalonamento.
	Vermelho	Crítico	O nó está conetado à grade, mas existe uma condição anormal que parou as operações normais. Você deve resolver o problema imediatamente.

A gravidade do alarme e o valor limite correspondente podem ser definidos para cada atributo numérico. O serviço NMS em cada nó Admin monitora continuamente os valores de atributo atuais em relação aos limites configurados. Quando um alarme é acionado, uma notificação é enviada a todos os funcionários designados.

Observe que um nível de gravidade normal não aciona um alarme.

Os valores de atributo são avaliados em relação à lista de alarmes ativados definidos para esse atributo. A lista de alarmes é verificada na seguinte ordem para encontrar a primeira classe de alarme com um alarme definido e ativado para o atributo:

1. Alarmes personalizados globais com severidades de alarme de crítico para Aviso.
2. Alarmes padrão com severidades de alarme de crítico para baixo para Aviso.

Depois que um alarme ativado para um atributo é encontrado na classe de alarme mais alta, o serviço NMS só é avaliado dentro dessa classe. O serviço NMS não será avaliado em relação às outras classes de menor prioridade. Ou seja, se houver um alarme personalizado global habilitado para um atributo, o serviço NMS somente avaliará o valor do atributo em relação aos alarmes personalizados globais. Os alarmes predefinidos não são avaliados. Assim, um alarme padrão habilitado para um atributo pode atender aos critérios necessários para acionar um alarme, mas ele não será acionado porque um alarme personalizado global (que não atende aos critérios especificados) para o mesmo atributo está ativado. Nenhum alarme é acionado e

nenhuma notificação é enviada.

Exemplo de acionamento de alarmes

Você pode usar este exemplo para entender como os alarmes personalizados globais e os alarmes padrão são acionados.

Para o exemplo a seguir, um atributo tem um alarme personalizado global e um alarme padrão definido e ativado como mostrado na tabela a seguir.

	Limiar de alarme personalizado global (ativado)	Limiar de alarme predefinido (ativado)
Aviso	1500	1000
Menor	15.000	1000
Maior	150.000	250.000

Se o atributo for avaliado quando seu valor for 1000, nenhum alarme será acionado e nenhuma notificação será enviada.

O alarme personalizado global tem precedência sobre o alarme predefinido. Um valor de 1000 não atinge o valor limite de qualquer nível de gravidade para o alarme Personalizado Global. Como resultado, o nível de alarme é avaliado como normal.

Após o cenário acima, se o alarme Global Custom estiver desativado, nada muda. O valor do atributo deve ser reavaliado antes de um novo nível de alarme ser acionado.

Com o alarme Global Custom desativado, quando o valor do atributo é reavaliado, o valor do atributo é avaliado em relação aos valores de limite para o alarme padrão. O nível de alarme aciona um alarme de nível de aviso e uma notificação por e-mail é enviada ao pessoal designado.

Alarmes da mesma gravidade

Se dois alarmes personalizados globais para o mesmo atributo tiverem a mesma gravidade, os alarmes serão avaliados com uma prioridade "de cima para baixo".

Por exemplo, se UMEM cair para 50MB, o primeiro alarme é acionado (50000000), mas não o abaixo dele (100000000).

Global Alarms
Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		

Se a ordem é invertida, quando UMEM cai para 100MB, o primeiro alarme (100000000) é acionado, mas não o abaixo dele (50000000).

Global Alarms
Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes

Notificações

Uma notificação relata a ocorrência de um alarme ou a mudança de estado de um serviço. As notificações de alarme podem ser enviadas por e-mail ou usando SNMP.

Para evitar que vários alarmes e notificações sejam enviados quando um valor limite de alarme é atingido, a gravidade do alarme é verificada em relação à gravidade atual do alarme para o atributo. Se não houver nenhuma mudança, então nenhuma outra ação é tomada. Isso significa que, à medida que o serviço NMS continua a monitorar o sistema, ele só irá disparar um alarme e enviar notificações na primeira vez que detetar uma condição de alarme para um atributo. Se um novo limite de valor para o atributo for atingido e detetado, a gravidade do alarme será alterada e uma nova notificação será enviada. Os alarmes são apagados quando as condições retornam ao nível normal.

O valor do gatilho mostrado na notificação de um estado de alarme é arredondado para três casas decimais. Portanto, um valor de atributo de 1,9999 aciona um alarme cujo limite é inferior a 2,0, embora a notificação de

alarme mostre o valor de gatilho como 2,0.

Novos serviços

À medida que novos serviços são adicionados através da adição de novos nós ou sites de grade, eles herdam alarmes padrão e alarmes personalizados globais.

Alarmes e tabelas

Os atributos de alarme exibidos nas tabelas podem ser desativados no nível do sistema. Os alarmes não podem ser desativados para linhas individuais em uma tabela.

Por exemplo, a tabela a seguir mostra dois alarmes de entradas críticas disponíveis (VMFI). (Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Storage Node*** > **SSM** > **Resources**.)

Você pode desativar o alarme VMFI para que o alarme VMFI de nível crítico não seja acionado (ambos os alarmes críticos atualmente aparecerão na tabela como verde); no entanto, você não pode desativar um único alarme em uma linha de tabela para que um alarme VMFI seja exibido como um alarme de nível crítico enquanto o outro permanece verde.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Reconhecer alarmes atuais (sistema legado)

Os alarmes herdados são acionados quando os atributos do sistema atingem os valores de limite de alarme. Opcionalmente, se você quiser reduzir ou limpar a lista de alarmes herdados, você pode reconhecer os alarmes.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter a permissão de reconhecer alarmes.

Sobre esta tarefa

Como o sistema de alarme antigo continua a ser suportado, a lista de alarmes legados na página Alarmes atuais é aumentada sempre que um novo alarme ocorre. Normalmente, pode ignorar os alarmes (porque os alertas fornecem uma melhor visualização do sistema) ou pode reconhecer os alarmes.

> Opcionalmente, quando você tiver feito a transição completa para o sistema de alerta, você pode desativar cada alarme legado para evitar que ele seja acionado e adicionado à contagem de alarmes legados.

Quando você reconhece um alarme, ele não está mais listado na página Alarmes atuais no Gerenciador de Grade, a menos que o alarme seja acionado no próximo nível de gravidade ou seja resolvido e ocorra novamente.

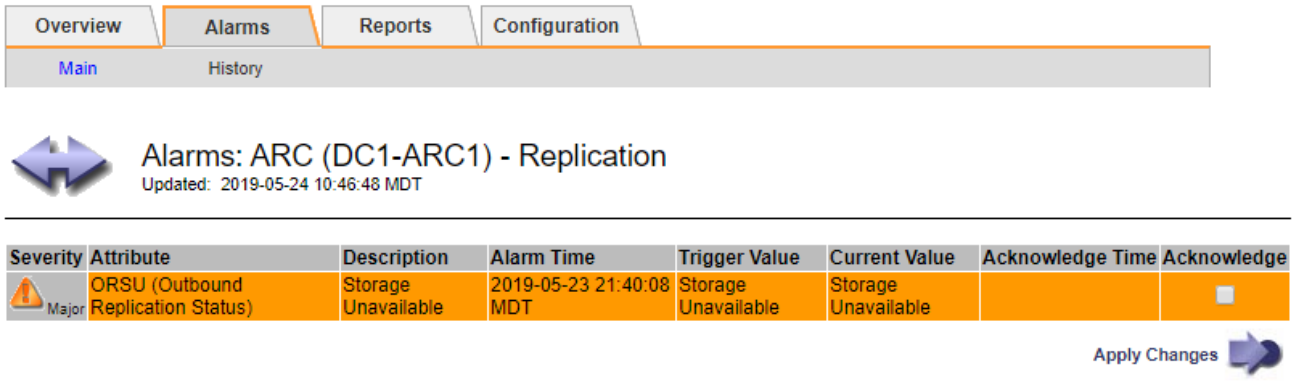
> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Current Alarmes**.

2. Selecione o nome do serviço na tabela.

   A guia Alarmes para o serviço selecionado é exibida (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarmes**).



3. Marque a caixa de seleção **Acknowledge** para o alarme e clique em **Apply Changes** (aplicar alterações).

   O alarme não aparece mais no painel ou na página Alarmes atuais.

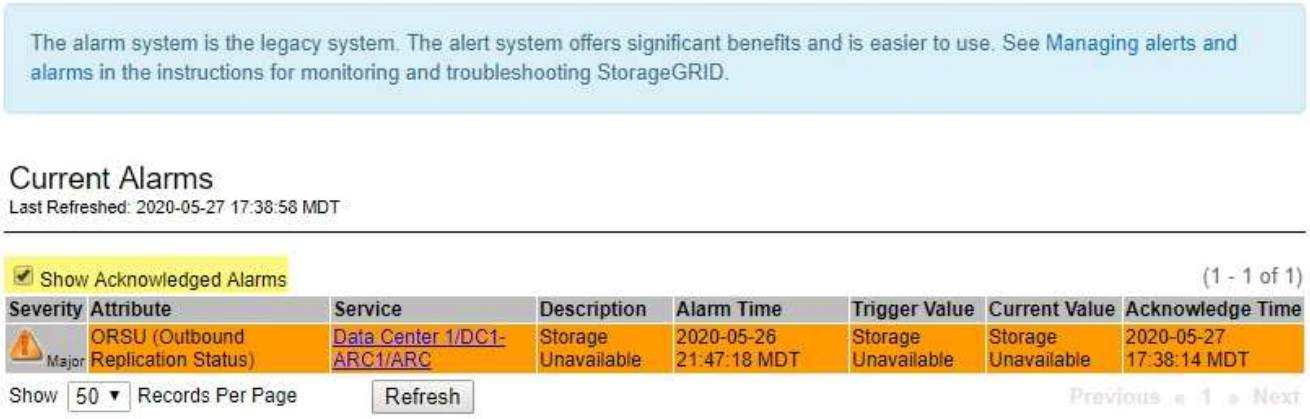
   > Quando você reconhece um alarme, a confirmação não é copiada para outros nós de administração. Por esse motivo, se você exibir o painel de outro nó Admin, poderá continuar a ver o alarme ativo.

4. Conforme necessário, visualize os alarmes reconhecidos.

   a. Selecione **SUPPORT** > **Alarmes (legacy)** > **Current Alarmes**.

   b. Selecione **Mostrar alarmes confirmados**.

      São apresentados quaisquer alarmes reconhecidos.



Exibir alarmes padrão (sistema legado)

Pode ver a lista de todos os alarmes herdados predefinidos.

Antes de começar

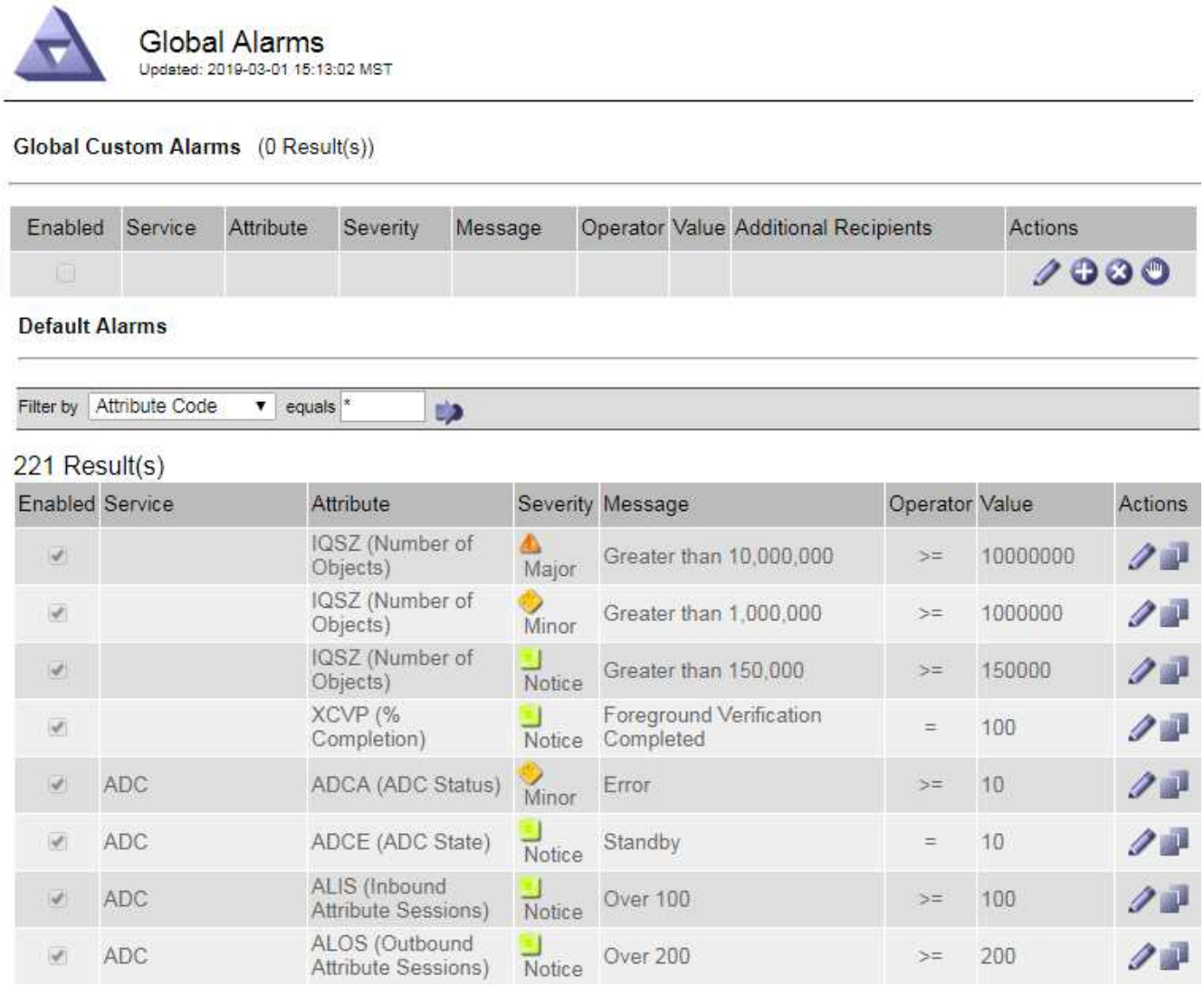
- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**.
2. Para Filtrar por, selecione **Código Atributo** ou **Nome Atributo**.
3. Para iguais, introduza um asterisco: `*`
4. Clique na seta ou pressione **Enter**.

   Todos os alarmes predefinidos estão listados.



Rever alarmes históricos e frequência de alarmes (sistema legado)

Ao solucionar um problema, você pode revisar a frequência com que um alarme legado foi acionado no passado.

Antes de começar

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

> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Passos

1. Siga estes passos para obter uma lista de todos os alarmes acionados durante um período de tempo.
   a. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes históricos**.
   b. Execute um dos seguintes procedimentos:
      - Clique num dos períodos de tempo.
      - Insira um intervalo personalizado e clique em **consulta personalizada**.

2. Siga estas etapas para descobrir a frequência com que alarmes foram acionados para um atributo específico.
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***grid node*** > ***Service ou Component*** > **Alarmes** > **History**.
   c. Selecione o atributo na lista.
   d. Execute um dos seguintes procedimentos:
      - Clique num dos períodos de tempo.
      - Insira um intervalo personalizado e clique em **consulta personalizada**.

      Os alarmes são listados em ordem cronológica inversa.
   e. Para retornar ao formulário de solicitação do histórico de alarmes, clique em **Histórico**.

Criar alarmes personalizados globais (sistema legado)

Você pode ter usado alarmes personalizados globais para o sistema legado para atender a requisitos específicos de monitoramento. Os alarmes personalizados globais podem ter níveis de alarme que substituem os alarmes padrão ou podem monitorar atributos que não têm um alarme padrão.

Antes de começar

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

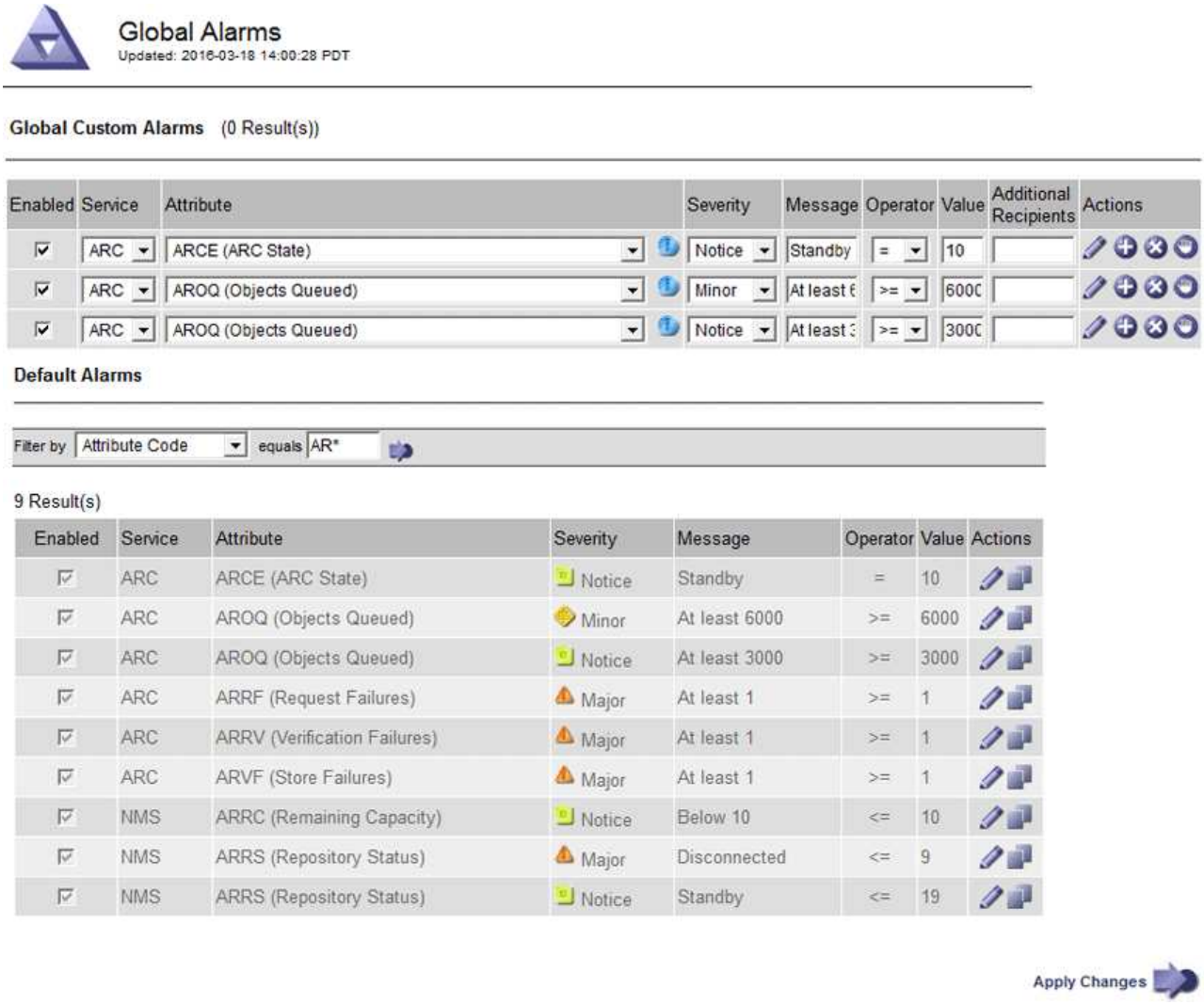
> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Os alarmes personalizados globais substituem os alarmes predefinidos. Você não deve alterar os valores de alarme padrão a menos que seja absolutamente necessário. Ao alterar os alarmes padrão, você corre o risco de ocultar problemas que, de outra forma, podem acionar um alarme.

> Tenha cuidado se alterar as definições de alarme. Por exemplo, se você aumentar o valor de limite para um alarme, talvez você não detete um problema subjacente. Discuta as alterações propostas com o suporte técnico antes de alterar uma definição de alarme.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**.
2. Adicione uma nova linha à tabela de alarmes personalizados globais:
   - Para adicionar um novo alarme, clique em **Edit** (Editar) (se esta for a primeira entrada) ou em **Insert** (Inserir) .



- Para modificar um alarme predefinido, procure o alarme predefinido.
  i. Em Filtrar por, selecione **Código Atributo** ou **Nome Atributo**.
  ii. Digite uma string de pesquisa.

  Especifique quatro carateres ou use carateres universais (por exemplo, A???? Ou AB*). Asteriscos (*) representam vários carateres, e os pontos de interrogação (?) representam um único caractere.

  iii. Clique na seta ou pressione **Enter**.
  iv. Na lista de resultados, clique em **Copiar** ao lado do alarme que deseja modificar.

  O alarme padrão é copiado para a tabela de alarmes personalizados globais.

3. Faça as alterações necessárias às definições de alarmes personalizados globais:

Rumo	Descrição
Ativado	Selecione ou desmarque a caixa de verificação para ativar ou desativar o alarme.

Rumo	Descrição
Atributo	Selecione o nome e o código do atributo que está sendo monitorado na lista de todos os atributos aplicáveis ao serviço ou componente selecionado. Para exibir informações sobre o atributo, clique em **Info** ao lado do nome do atributo.
Gravidade	O ícone e o texto que indicam o nível do alarme.
Mensagem	O motivo do alarme (perda de conexão, espaço de armazenamento abaixo de 10%, e assim por diante).
Operador	Operadores para testar o valor do atributo atual em relação ao limite do valor: • igual a • > superior a. • inferior a. • > superior ou igual a • menos ou igual a • ≠ não é igual a
Valor	O valor limite do alarme usado para testar o valor real do atributo usando o operador. A entrada pode ser um único número, um intervalo de números especificado com dois pontos (1:3) ou uma lista delimitada por vírgulas de números e intervalos.
Destinatários adicionais	Uma lista suplementar de endereços de e-mail a notificar quando o alarme é acionado. Isso é além da lista de e-mails configurada na página **Alarmes** > **Configuração de e-mail**. As listas são delineadas por vírgulas. **Observação:** listas de discussão exigem configuração do servidor SMTP para operar. Antes de adicionar listas de discussão, confirme se o SMTP está configurado. As notificações de alarmes personalizados podem substituir as notificações de alarmes personalizados globais ou predefinidos.
Ações	Botões de controle para: Editar uma linha Insira uma linha Elimine uma linha Arraste uma linha para cima ou para baixo Copie uma linha

4. Clique em **aplicar alterações**.

Desativar alarmes (sistema legado)

Os alarmes no sistema de alarme legado são ativados por padrão, mas você pode desativar os alarmes que não são necessários. Você também pode desativar os alarmes herdados depois de fazer a transição completa para o novo sistema de alerta.

> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Desativar um alarme predefinido (sistema legado)

Você pode desativar um dos alarmes padrão herdados para todo o sistema.

Antes de começar

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

Sobre esta tarefa

Desativar um alarme para um atributo que atualmente tem um alarme acionado não limpa o alarme atual. O alarme será desativado na próxima vez que o atributo cruzar o limite do alarme, ou você poderá apagar o alarme acionado.

> Não desative nenhum dos alarmes herdados até que você tenha feito a transição completa para o novo sistema de alerta. Caso contrário, você pode não detetar um problema subjacente até que ele tenha impedido uma operação crítica de ser concluída.

Passos

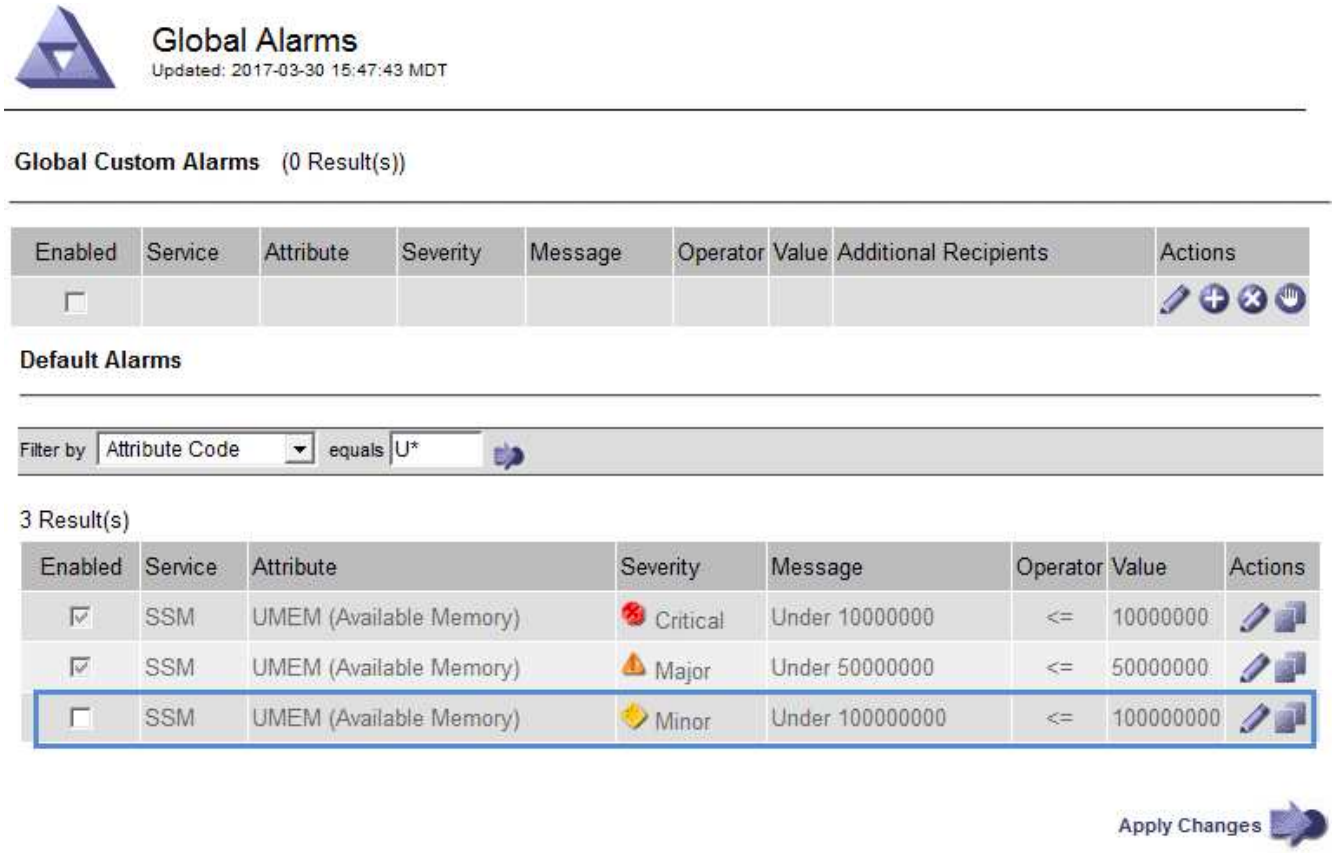
1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**.
2. Procure o alarme predefinido para desativar.
   a. Na seção Alarmes padrão, selecione **Filtrar por** > **Código de Atributo** ou **Nome do Atributo**.
   b. Digite uma string de pesquisa.

      Especifique quatro carateres ou use carateres universais (por exemplo, A???? Ou AB*). Asteriscos (*) representam vários carateres, e os pontos de interrogação (?) representam um único caractere.

   c. Clique na seta ou pressione **Enter**.

      > A seleção de **Defaults Disabled** exibe uma lista de todos os alarmes predefinidos atualmente desativados.

3. Na tabela de resultados da pesquisa, clique no ícone Editar para o alarme que deseja desativar.



A caixa de verificação **Enabled** para o alarme selecionado fica ativa.

4. Desmarque a caixa de seleção **Enabled**.
5. Clique em **aplicar alterações**.

   O alarme predefinido está desativado.

Desativar alarmes personalizados globais (sistema legado)

Você pode desativar um alarme personalizado global legado para todo o sistema.

Antes de começar

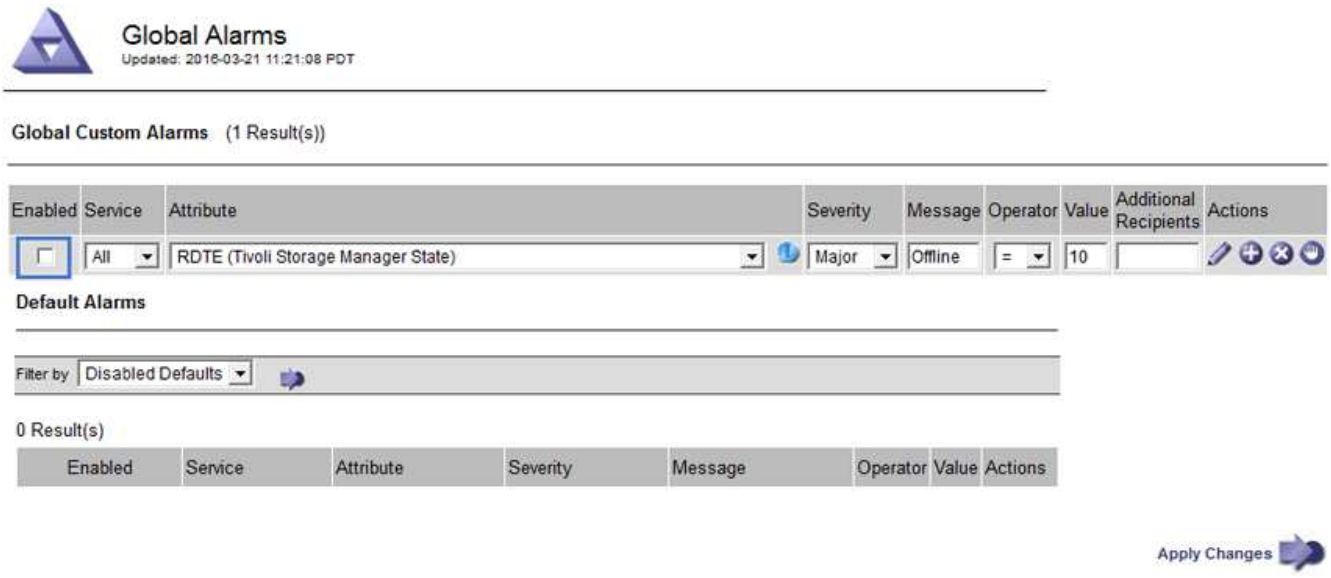
- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

Desativar um alarme para um atributo que atualmente tem um alarme acionado não limpa o alarme atual. O alarme será desativado na próxima vez que o atributo cruzar o limite do alarme, ou você poderá apagar o alarme acionado.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Alarmes globais**.
2. Na tabela Alarmes personalizados globais, clique em **Editar** ao lado do alarme que deseja desativar.
3. Desmarque a caixa de seleção **Enabled**.



4. Clique em **aplicar alterações**.

   O alarme personalizado global está desativado.

Apagar alarmes acionados (sistema legado)

Se um alarme legado for acionado, você pode limpá-lo em vez de reconhecê-lo.

Antes de começar

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

Desativar um alarme para um atributo que atualmente tem um alarme acionado contra ele não limpa o alarme. O alarme será desativado na próxima vez que o atributo for alterado. Você pode reconhecer o alarme ou, se quiser apagar imediatamente o alarme em vez de esperar que o valor do atributo seja alterado (resultando em uma alteração no estado do alarme), você pode apagar o alarme acionado. Você pode achar isso útil se quiser limpar um alarme imediatamente contra um atributo cujo valor não muda frequentemente (por exemplo, atributos de estado).

1. Desative o alarme.
2. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: *`ssh admin@primary_Admin_Node_IP`*
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

3. Reinicie o serviço NMS: `service nms restart`
4. Terminar sessão no nó Admin: `exit`

   O alarme é apagado.

Configurar notificações para alarmes (sistema legado)

O sistema StorageGRID pode enviar automaticamente e-mails e "Notificações SNMP" quando um alarme é acionado ou um estado de serviço muda.

Por padrão, as notificações por e-mail de alarme não são enviadas. Para notificações de e-mail, você deve configurar o servidor de e-mail e especificar os destinatários de e-mail. Para notificações SNMP, você deve configurar o agente SNMP.

Tipos de notificações de alarme (sistema legado)

Quando um alarme legado é acionado, o sistema StorageGRID envia dois tipos de notificações de alarme: Nível de gravidade e estado de serviço.

Notificações de nível de gravidade

Uma notificação por e-mail de alarme é enviada quando um alarme legado é acionado em um nível de gravidade selecionado:

- Aviso
- Menor
- Maior
- Crítico

Uma lista de correio recebe todas as notificações relacionadas com o alarme para a gravidade selecionada. Uma notificação também é enviada quando o alarme sai do nível de alarme — seja por ser resolvido ou inserindo um nível de gravidade de alarme diferente.

Notificações do estado do serviço

Uma notificação de estado do serviço é enviada quando um serviço (por exemplo, o serviço LDR ou o serviço NMS) entra no estado do serviço selecionado e quando sai do estado do serviço selecionado. As notificações de estado do serviço são enviadas quando um serviço entra ou deixa um dos seguintes estados de serviço:

- Desconhecido
- Administrativamente para baixo

Uma lista de discussão recebe todas as notificações relacionadas a alterações no estado selecionado.

Configurar as definições do servidor de correio eletrónico para alarmes (sistema legado)

Se você quiser que o StorageGRID envie notificações por e-mail quando um alarme legado for acionado, especifique as configurações do servidor de e-mail SMTP. O sistema StorageGRID envia apenas e-mail; ele não pode receber e-mails.

Antes de começar

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

Sobre esta tarefa

Use essas configurações para definir o servidor SMTP usado para notificações de e-mail de alarme herdadas e mensagens de e-mail do AutoSupport. Essas configurações não são usadas para notificações de alerta.

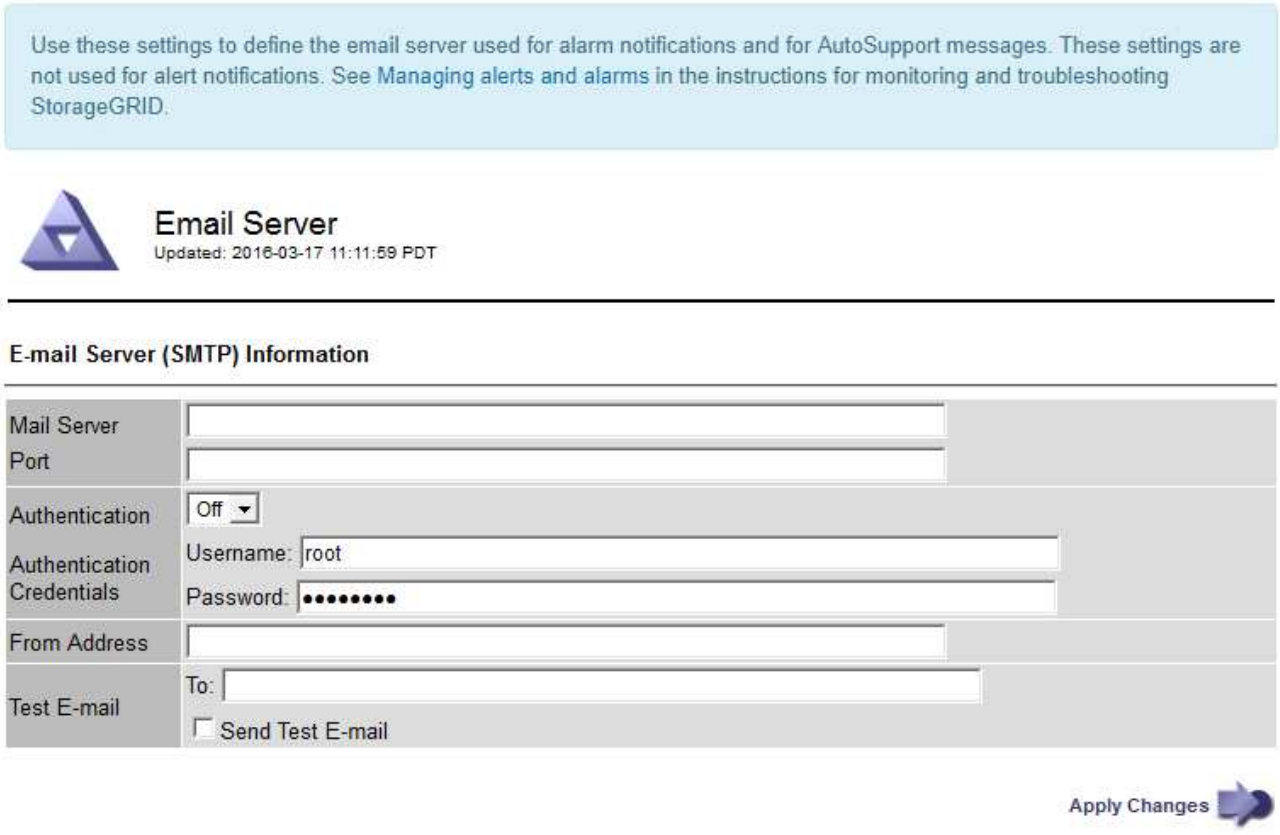
Se você usar SMTP como protocolo para pacotes AutoSupport, talvez você já tenha configurado um servidor de email SMTP. O mesmo servidor SMTP é usado para notificações de e-mail de alarme, para que você possa ignorar este procedimento. Consulte "Instruções para administrar o StorageGRID".

SMTP é o único protocolo suportado para enviar e-mails.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**.
2. No menu e-mail, selecione **servidor**.

   A página servidor de e-mail é exibida. Esta página também é usada para configurar o servidor de e-mail para pacotes AutoSupport.



3. Adicione as seguintes definições do servidor de correio SMTP:

Item	Descrição
Servidor de correio	Endereço IP do servidor de correio SMTP. Você pode inserir um nome de host em vez de um endereço IP se tiver configurado as configurações de DNS anteriormente no nó Admin.
Porta	Número da porta para aceder ao servidor de correio SMTP.
Autenticação	Permite a autenticação do servidor de correio SMTP. Por padrão, a autenticação está desativada.

Item	Descrição
Credenciais de autenticação	Nome de utilizador e palavra-passe do servidor de correio SMTP. Se a Autenticação estiver definida como ativada, um nome de usuário e senha para acessar o servidor de e-mail SMTP devem ser fornecidos.

4. Em **de Endereço**, insira um endereço de e-mail válido que o servidor SMTP reconhecerá como endereço de e-mail de envio. Este é o endereço de e-mail oficial a partir do qual a mensagem de e-mail é enviada.
5. Opcionalmente, envie um e-mail de teste para confirmar se as configurações do servidor de e-mail SMTP estão corretas.
   a. Na caixa **Teste e-mail** > **para**, adicione um ou mais endereços que você possa acessar.

      Você pode inserir um único endereço de e-mail ou uma lista delimitada por vírgulas de endereços de e-mail. Como o serviço NMS não confirma sucesso ou falha quando um e-mail de teste é enviado, você deve ser capaz de verificar a caixa de entrada do destinatário do teste.

   b. Selecione **Enviar e-mail de teste**.
6. Clique em **aplicar alterações**.

   As definições do servidor de correio SMTP são guardadas. Se você inseriu informações para um e-mail de teste, esse e-mail será enviado. Os e-mails de teste são enviados para o servidor de e-mail imediatamente e não são enviados através da fila de notificações. Em um sistema com vários nós de administração, cada nó de administração envia um e-mail. O recebimento do e-mail de teste confirma que as configurações do servidor de e-mail SMTP estão corretas e que o serviço NMS está se conetando com êxito ao servidor de e-mail. Um problema de conexão entre o serviço NMS e o servidor de e-mail aciona o alarme MINS (NMS Notification Status) legado no nível de gravidade menor.

Criar modelos de e-mail de alarme (sistema legado)

Os modelos de e-mail permitem personalizar o cabeçalho, o rodapé e a linha de assunto de uma notificação por e-mail de alarme legado. Você pode usar modelos de e-mail para enviar notificações exclusivas que contêm o mesmo corpo de texto para diferentes listas de discussão.

Antes de começar

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

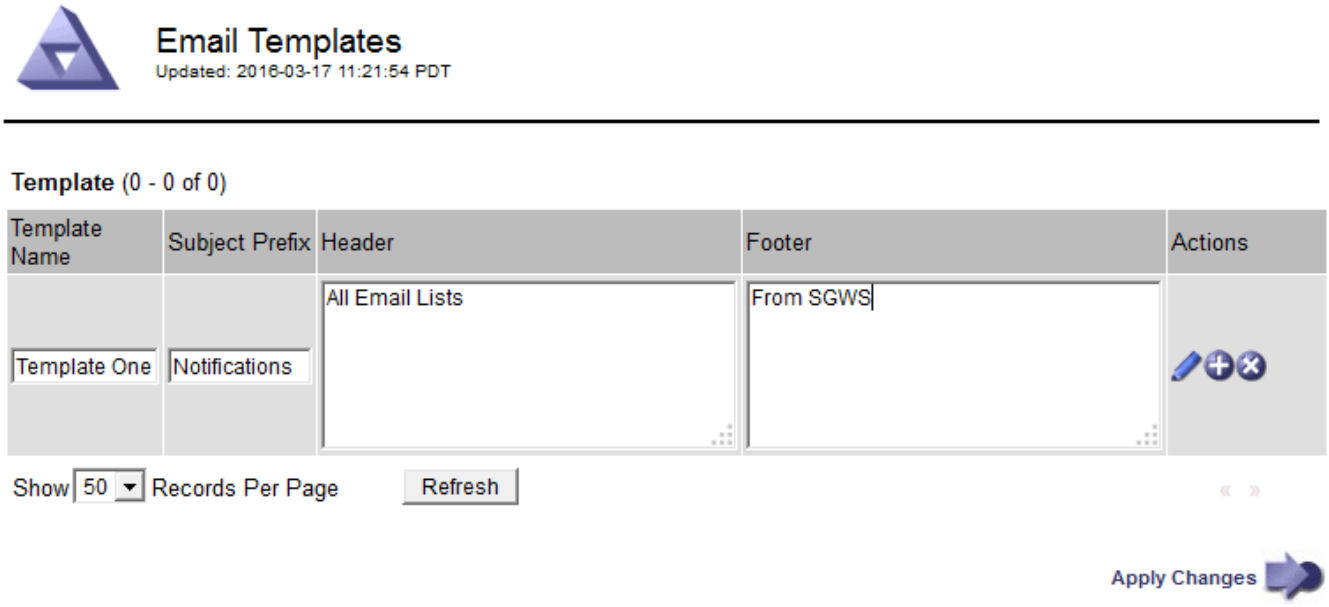
Sobre esta tarefa

Use essas configurações para definir os modelos de e-mail usados para notificações de alarme herdadas. Essas configurações não são usadas para notificações de alerta.

Listas de discussão diferentes podem exigir informações de Contato diferentes. Os modelos não incluem o texto do corpo da mensagem de e-mail.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**.
2. No menu e-mail, selecione **modelos**.
3. Clique em **Edit** (ou **Insert** se este não for o primeiro modelo).



4. Na nova linha, adicione o seguinte:

Item	Descrição
Nome do modelo	Nome exclusivo utilizado para identificar o modelo. Os nomes dos modelos não podem ser duplicados.
Prefixo do assunto	Opcional. Prefixo que aparecerá no início da linha de assunto de um email. Prefixos podem ser usados para configurar facilmente filtros de e-mail e organizar notificações.
Colhedor	Opcional. Texto do cabeçalho que aparece no início do corpo da mensagem de e-mail. O texto do cabeçalho pode ser usado para prefácio do conteúdo da mensagem de e-mail com informações como nome e endereço da empresa.
Rodapé	Opcional. Texto de rodapé que aparece no final do corpo da mensagem de e-mail. O texto do rodapé pode ser usado para fechar a mensagem de e-mail com informações de lembrete, como um número de telefone de Contato ou um link para um site da Web.

5. Clique em **aplicar alterações**.

   Um novo modelo para notificações é adicionado.

Criar listas de discussão para notificações de alarme (sistema legado)

As listas de discussão permitem que você notifique os destinatários quando um alarme legado é acionado ou quando um estado de serviço muda. Você deve criar pelo menos uma lista de discussão antes que qualquer notificação por e-mail de alarme possa ser enviada. Para enviar uma notificação para um único destinatário, crie uma lista de discussão com um endereço de e-mail.

Antes de começar

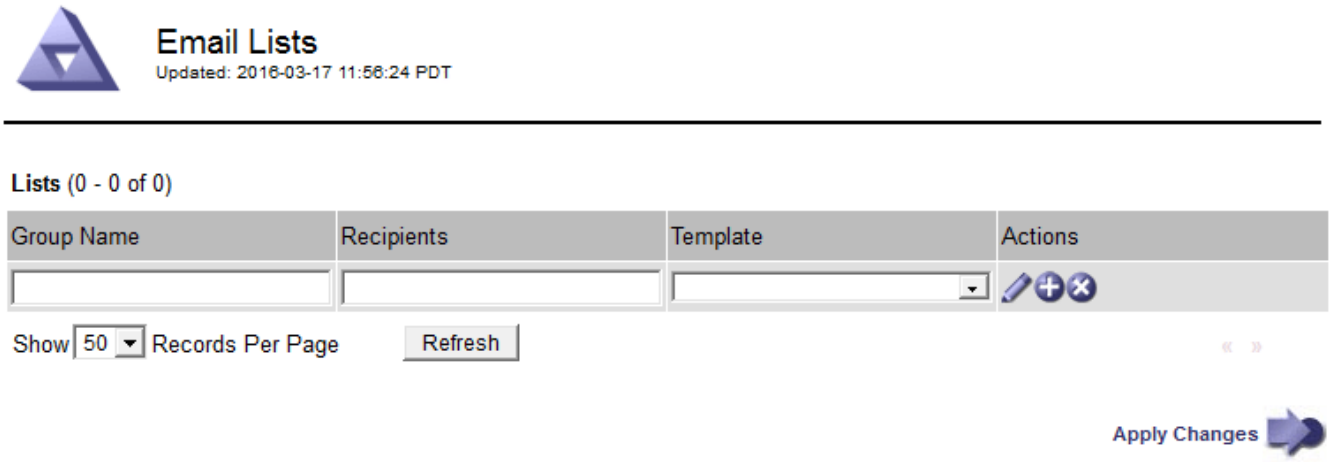
- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Se você quiser especificar um modelo de e-mail para a lista de e-mail (cabeçalho personalizado, rodapé e linha de assunto), você já deve ter criado o modelo.

Sobre esta tarefa

Use essas configurações para definir as listas de discussão usadas para notificações de e-mail de alarme herdadas. Essas configurações não são usadas para notificações de alerta.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**.
2. No menu e-mail, selecione **listas**.
3. Clique em **Edit** (ou *Insert* se esta não for a primeira lista de discussão).



4. Na nova linha, adicione o seguinte:

Item	Descrição
Nome do grupo	Nome exclusivo usado para identificar a lista de discussão. Os nomes da lista de discussão não podem ser duplicados. **Observação:** se você alterar o nome de uma lista de discussão, a alteração não será propagada para os outros locais que usam o nome da lista de discussão. Você deve atualizar manualmente todas as notificações configuradas para usar o novo nome da lista de discussão.
Destinatários	Um único endereço de e-mail, uma lista de e-mail configurada anteriormente ou uma lista delimitada por vírgulas de endereços de e-mail e listas de e-mail para as quais as notificações serão enviadas. **Observação:** se um endereço de e-mail pertencer a várias listas de e-mail, somente uma notificação de e-mail será enviada quando um evento de acionamento de notificação ocorrer.

Item	Descrição
Modelo	Opcionalmente, selecione um modelo de e-mail para adicionar um cabeçalho, rodapé e linha de assunto exclusivos às notificações enviadas a todos os destinatários desta lista de e-mail.

5. Clique em **aplicar alterações**.

   Uma nova lista de discussão é criada.

Configurar notificações por e-mail para alarmes (sistema legado)

Para receber notificações por e-mail para o sistema de alarme legado, os destinatários devem ser membros de uma lista de discussão e essa lista deve ser adicionada à página notificações. As notificações são configuradas para enviar e-mails aos destinatários somente quando um alarme com um nível de gravidade especificado é acionado ou quando um estado de serviço muda. Assim, os destinatários só recebem as notificações que precisam receber.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você deve ter configurado uma lista de e-mail.

Sobre esta tarefa

Use essas configurações para configurar notificações para alarmes legados. Essas configurações não são usadas para notificações de alerta.

Se um endereço de e-mail (ou lista) pertencer a várias listas de e-mail, somente uma notificação de e-mail será enviada quando um evento de acionamento de notificação ocorrer. Por exemplo, um grupo de administradores na sua organização pode ser configurado para receber notificações de todos os alarmes, independentemente da gravidade. Outro grupo pode exigir notificações apenas para alarmes com uma gravidade crítica. Você pode pertencer a ambas as listas. Se um alarme crítico for acionado, você receberá apenas uma notificação.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**.
2. No menu e-mail, selecione **notificações**.
3. Clique em *Edit* (ou *Insert* se esta não for a primeira notificação).
4. Em Lista de e-mail, selecione a lista de discussão.
5. Selecione um ou mais níveis de gravidade de alarme e estados de serviço.
6. Clique em **aplicar alterações**.

   As notificações serão enviadas para a lista de discussão quando os alarmes com o nível de gravidade de alarme ou estado de serviço selecionado forem acionados ou alterados.

Suprimir notificações de alarme para uma lista de discussão (sistema legado)

Você pode suprimir notificações de alarme para uma lista de discussão quando não quiser mais que a lista de discussão receba notificações sobre alarmes. Por exemplo, você pode querer suprimir notificações sobre

alarmes legados depois de fazer a transição para o uso de notificações por e-mail de alerta.

Antes de começar

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

Utilize estas definições para suprimir as notificações por e-mail do sistema de alarme antigo. Essas configurações não se aplicam às notificações de alerta por e-mail.

> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**.
2. No menu e-mail, selecione **notificações**.
3. Clique em **Editar** ao lado da lista de discussão para a qual você deseja suprimir notificações.
4. Em suprimir, marque a caixa de seleção ao lado da lista de discussão que deseja suprimir ou selecione **suprimir** na parte superior da coluna para suprimir todas as listas de discussão.
5. Clique em **aplicar alterações**.

   As notificações de alarme herdadas são suprimidas para as listas de discussão selecionadas.

Ver alarmes legados

Os alarmes (sistema legado) são acionados quando os atributos do sistema atingem os valores de limite de alarme. Pode visualizar os alarmes atualmente ativos a partir da página Alarmes atuais.

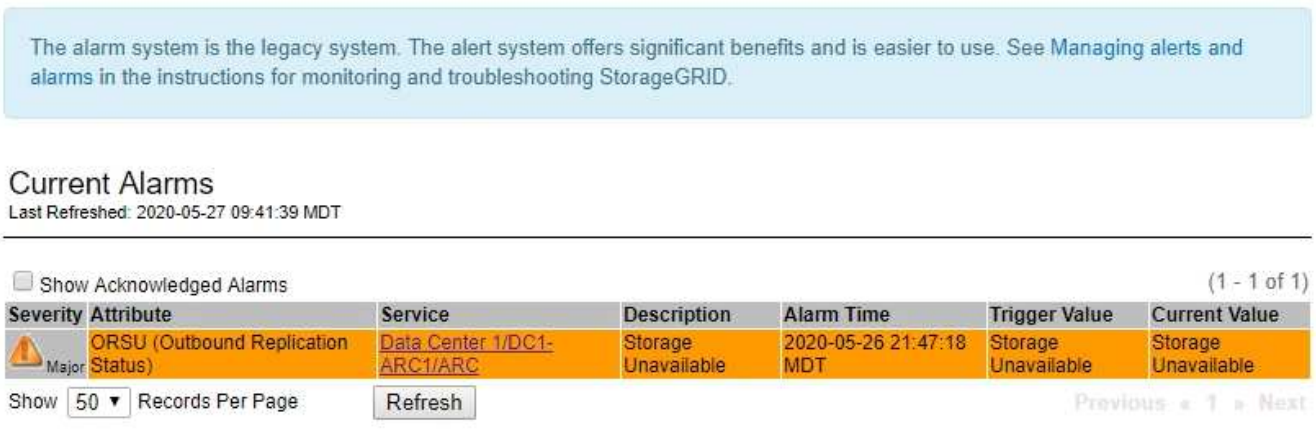
> Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Antes de começar

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

Passos

1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Current Alarmes**.

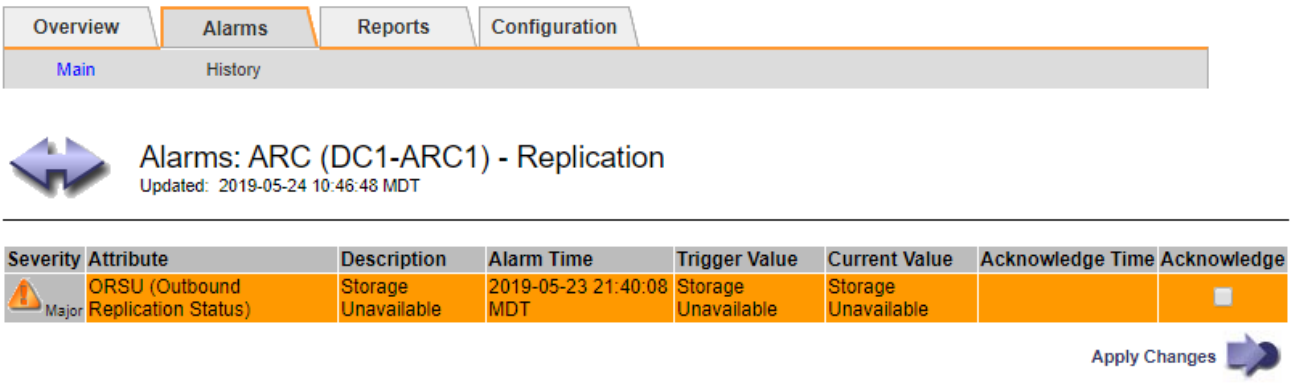


O ícone de alarme indica a gravidade de cada alarme, da seguinte forma:

Ícone	Cor	Gravidade do alarme	Significado
	Amarelo	Aviso	O nó está conetado à grade, mas existe uma condição incomum que não afeta as operações normais.
	Laranja claro	Menor	O nó está conetado à grade, mas existe uma condição anormal que pode afetar a operação no futuro. Você deve investigar para evitar o escalonamento.
	Laranja escuro	Maior	O nó está conetado à grade, mas existe uma condição anormal que afeta atualmente a operação. Isso requer atenção imediata para evitar o escalonamento.
	Vermelho	Crítico	O nó está conetado à grade, mas existe uma condição anormal que parou as operações normais. Você deve resolver o problema imediatamente.

2. Para saber mais sobre o atributo que fez com que o alarme fosse acionado, clique com o botão direito do Mouse no nome do atributo na tabela.
3. Para ver detalhes adicionais sobre um alarme, clique no nome do serviço na tabela.

   A guia Alarmes para o serviço selecionado é exibida (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarmes**).



4. Se você quiser limpar a contagem de alarmes atuais, você pode, opcionalmente, fazer o seguinte:
   - Confirme o alarme. Um alarme reconhecido não é mais incluído na contagem de alarmes herdados, a menos que seja acionado no próximo nível de gravidade ou seja resolvido e ocorra novamente.
   - Desative um alarme padrão específico ou um alarme personalizado global para todo o sistema para evitar que ele seja acionado novamente.

Informações relacionadas

"Referência de alarmes (sistema legado)"

"Reconhecer alarmes atuais (sistema legado)"

"Desativar alarmes (sistema legado)"

Referência de alarmes (sistema legado)

A tabela a seguir lista todos os alarmes padrão herdados. Se um alarme for acionado, você pode procurar o código de alarme nesta tabela para encontrar as ações recomendadas.

Embora o sistema de alarme antigo continue a ser suportado, o sistema de alerta oferece benefícios significativos e é mais fácil de usar.

Código	Nome	Serviço	Ação recomendada
ABRL	Relés Atributo disponíveis	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Restaure a conetividade a um serviço (um serviço ADC) executando um serviço de relé de atributos o mais rápido possível. Se não houver relés de atributos conetados, o nó de grade não poderá relatar valores de atributo ao serviço NMS. Assim, o serviço NMS não pode mais monitorar o status do serviço ou atualizar atributos para o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
ACMS	Serviços de metadados disponíveis	BARC, BLDR, BCMN	Um alarme é acionado quando um serviço LDR ou ARC perde a ligação a um serviço DDS. Se isso ocorrer, as transações de ingestão ou recuperação não podem ser processadas. Se a indisponibilidade dos serviços DDS for apenas um breve problema transitório, as transações podem ser atrasadas. Verifique e restaure as ligações a um serviço DDS para apagar este alarme e devolver o serviço à funcionalidade completa.

Código	Nome	Serviço	Ação recomendada
ATUA	Status de serviço do Cloud Tiering	ARCO	Disponível apenas para nós de arquivamento com um tipo de destino de disposição em camadas na nuvem - Simple Storage Service (S3). Se o atributo ACTS para o nó de arquivo estiver definido como somente leitura ativado ou leitura-escrita Desativado, você deverá definir o atributo como leitura-escrita habilitado. Se um alarme principal for acionado devido a uma falha de autenticação, verifique as credenciais associadas ao intervalo de destino e atualize os valores, se necessário. Se um alarme principal for acionado devido a qualquer outro motivo, contacte o suporte técnico.
ADCA	Estado ADC	ADC	Se um alarme for acionado, selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ADC** > **Overview** > **Main** e **ADC** > **Alarmes** > **Main** para determinar a causa do alarme. Se o problema persistir, entre em Contato com o suporte técnico.
ADCE	Estado ADC	ADC	Se o valor do Estado ADC for Standby, continue monitorando o serviço e, se o problema persistir, entre em Contato com o suporte técnico. Se o valor de ADC State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
AITE	Recuperar Estado	BARC	Disponível apenas para nós de arquivo com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor de Retrieve State estiver aguardando o Target, verifique o servidor de middleware TSM e certifique-se de que ele está funcionando corretamente. Se o nó de arquivo tiver sido adicionado ao sistema StorageGRID, certifique-se de que a ligação do nó de arquivo ao sistema de armazenamento de arquivos externo visado está configurada corretamente. Se o valor do Estado de recuperação de Arquivo for Offline, tente atualizar o estado para Online. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, selecione **Archive Retrieve State** > **Online** e clique em **Apply Changes**. Se o problema persistir, entre em Contato com o suporte técnico.
AITU	Recuperar Estado	BARC	Se o valor de Retrieve Status for Target Error, verifique se há erros no sistema de armazenamento de arquivos externo de destino. Se o valor de Archive Retrieve Status (Estado de recuperação de arquivo) for Session Lost (perda de sessão), verifique o sistema de armazenamento de arquivo externo alvo para garantir que está online e a funcionar corretamente. Verifique a conexão de rede com o destino. Se o valor do Estado de recuperação de Arquivo for erro desconhecido, contacte o suporte técnico.
ALIS	Sessões Atributo inbound	ADC	Se o número de sessões de atributo de entrada em um relay de atributo crescer muito grande, pode ser uma indicação de que o sistema StorageGRID ficou desequilibrado. Em condições normais, as sessões de atributos devem ser distribuídas uniformemente entre os serviços ADC. Um desequilíbrio pode levar a problemas de desempenho. Se o problema persistir, entre em Contato com o suporte técnico.
ALOS	Sessões de Atributo de saída	ADC	O serviço ADC tem um alto número de sessões de atributos e está se tornando sobrecarregado. Se este alarme for acionado, contacte a assistência técnica.

Código	Nome	Serviço	Ação recomendada
ALUR	Repositórios Atributo inalcançáveis	ADC	Verifique a conetividade de rede com o serviço NMS para garantir que o serviço possa entrar em Contato com o repositório de atributos. Se este alarme for acionado e a conetividade de rede estiver boa, contacte o suporte técnico.
AMQS	Mensagens de auditoria enfileiradas	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se as mensagens de auditoria não puderem ser encaminhadas imediatamente para um reencaminhamento ou repositório de auditoria, as mensagens serão armazenadas em uma fila de discos. Se a fila de discos ficar cheia, podem ocorrer interrupções. Para permitir que você responda a tempo para evitar uma interrupção, os alarmes AMQS são acionados quando o número de mensagens na fila de discos atinge os seguintes limites: • Aviso: Mais de 100.000 mensagens • Menor: Pelo menos 500.000 mensagens • Maior: Pelo menos 2.000.000 mensagens • Crítico: Pelo menos 5.000.000 mensagens Se um alarme AMQS for acionado, verifique a carga no sistema - se houver um número significativo de transações, o alarme deve resolver-se ao longo do tempo. Neste caso, pode ignorar o alarme. Se o alarme persistir e aumentar a 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 erro ou Desativado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Código	Nome	Serviço	Ação recomendada
AOTE	Estado da loja	BARC	Disponível apenas para nós de arquivo com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do Estado de armazenamento estiver a aguardar o destino, verifique o sistema de armazenamento de arquivos externo e certifique-se de que está a funcionar corretamente. Se o nó de arquivo tiver sido adicionado ao sistema StorageGRID, certifique-se de que a ligação do nó de arquivo ao sistema de armazenamento de arquivos externo visado está configurada corretamente. Se o valor de Estado da loja estiver offline, verifique o valor de Estado da loja. Corrija quaisquer problemas antes de mover o estado da loja de volta para Online.
AOTU	Estado da loja	BARC	Se o valor de Status da Loja for sessão perdida, verifique se o sistema de armazenamento de arquivos externo está conetado e on-line. Se o valor de Target Error (erro de destino), verifique se há erros no sistema de armazenamento de arquivos externo. Se o valor do Status da Loja for erro desconhecido, entre em Contato com o suporte técnico.
APMS	Conetividade Multipath de armazenamento	SSM	Se o alarme de estado de multipath aparecer como "degradado" (selecione **SUPPORT** > **Tools** > **Grid topology**, selecione ***site*** > ***grid node*** > **SSM** > **Events**), faça o seguinte: 1. Conete ou substitua o cabo que não exibe nenhuma luz indicadora. 2. Aguarde de um a cinco minutos. Não desligue o outro cabo até, pelo menos, cinco minutos depois de ligar o primeiro. Desconetar muito cedo pode fazer com que o volume raiz se torne somente leitura, o que requer que o hardware seja reiniciado. 3. Retorne à página **SSM** > **recursos** e verifique se o status do Multipath "degradado" foi alterado para "nominal" na seção hardware de armazenamento.

Código	Nome	Serviço	Ação recomendada
ARCE	ESTADO do ARCO	ARCO	O serviço ARC tem um estado de espera até que todos os componentes ARC (replicação, armazenamento, recuperação, destino) tenham iniciado. Ele então faz a transição para Online. Se o valor do estado ARC não passar de Standby para Online, verifique o estado dos componentes ARC. Se o valor de ARC State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
AROQ	Objetos em fila de espera	ARCO	Este alarme pode ser acionado se o dispositivo de armazenamento amovível estiver a funcionar lentamente devido a problemas com o sistema de armazenamento de arquivos externo visado ou se encontrar vários erros de leitura. Verifique se há erros no sistema de armazenamento de arquivos externo e verifique se ele está funcionando corretamente. Em alguns casos, esse erro pode ocorrer como resultado de uma alta taxa de solicitações de dados. Monitore o número de objetos enfileirados à medida que a atividade do sistema diminui.

Código	Nome	Serviço	Ação recomendada
ARRF	Falhas de solicitação	ARCO	Se uma recuperação do sistema de armazenamento de arquivos externo visado falhar, o nó de arquivo tentará novamente a recuperação, pois a falha pode ser devido a um problema transitório. No entanto, se os dados do objeto estiverem corrompidos ou tiverem sido marcados como estando permanentemente indisponíveis, a recuperação não falhará. Em vez disso, o nó de arquivo tenta continuamente a recuperação e o valor para falhas de solicitação continua a aumentar. Este alarme pode indicar que o suporte de armazenamento que contém os dados solicitados está corrompido. Verifique o sistema de armazenamento de arquivos externo para diagnosticar ainda mais o problema. Se você determinar que os dados do objeto não estão mais no arquivo, o objeto terá que ser removido do sistema StorageGRID. Para obter mais informações, entre em Contato com o suporte técnico. Assim que o problema que acionou este alarme for resolvido, reponha a contagem de avarias. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, selecione **Reset Request Failure Count** e clique em **Apply Changes**.
ARRV	Falhas de verificação	ARCO	Para diagnosticar e corrigir esse problema, entre em Contato com o suporte técnico. Depois de resolver o problema que acionou este alarme, reponha a contagem de avarias. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, selecione **Reset Verification Failure Count** e clique em **Apply Changes**.

Código	Nome	Serviço	Ação recomendada
ARVF	Falhas de armazenamento	ARCO	Este alarme pode ocorrer como resultado de erros com o sistema de armazenamento de arquivos externo visado. Verifique se há erros no sistema de armazenamento de arquivos externo e verifique se ele está funcionando corretamente. Assim que o problema que acionou este alarme for resolvido, reponha a contagem de avarias. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, selecione **Reset Store Failure Count** e clique em **Apply Changes**.
ASXP	Compartilhamentos de auditoria	AMS	Um alarme é acionado se o valor de compartilhamentos de auditoria for desconhecido. Este alarme pode indicar um problema com a instalação ou configuração do nó Admin. Se o problema persistir, entre em Contato com o suporte técnico.
AUMA	Estado AMS	AMS	Se o valor do Status AMS for DB Connectivity Error (erro de conetividade de banco de dados), reinicie o nó da grade. Se o problema persistir, entre em Contato com o suporte técnico.
AUME	Estado AMS	AMS	Se o valor do estado AMS for em espera, continue a monitorizar o sistema StorageGRID. Se o problema persistir, entre em Contato com o suporte técnico. Se o valor do Estado AMS for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
AUXS	Estado exportação Auditoria	AMS	Se um alarme for acionado, corrija o problema subjacente e reinicie o serviço AMS. Se o problema persistir, entre em Contato com o suporte técnico.
BADD	Falha na contagem de unidades do controlador de armazenamento	SSM	Este alarme é acionado quando uma ou mais unidades de um dispositivo StorageGRID falharam ou não são ideais. Substitua as unidades conforme necessário.

Código	Nome	Serviço	Ação recomendada
BASF	Identificadores de Objeto disponíveis	CMN	Quando um sistema StorageGRID é provisionado, o serviço CMN recebe um número fixo de identificadores de objeto. Este alarme é acionado quando o sistema StorageGRID começa a esgotar o seu fornecimento de identificadores de objetos. Para alocar mais identificadores, entre em Contato com o suporte técnico.
GRAVES	Estado Alocação bloco Identificador	CMN	Por padrão, um alarme é acionado quando os identificadores de objeto não podem ser alocados porque o quórum de ADC não pode ser alcançado. A alocação de bloco de identificador no serviço CMN requer um quorum (50% mais 1) dos serviços ADC para estar on-line e conetado. Se o quórum não estiver disponível, o serviço CMN não poderá alocar novos blocos de identificador até que o quórum ADC seja restabelecido. Se o quórum de ADC for perdido, geralmente não há impactos imediato no sistema StorageGRID (os clientes ainda podem ingerir e recuperar conteúdo), já que aproximadamente um mês de fornecimento de identificadores são armazenados em cache em outro lugar na grade; no entanto, se a condição continuar, o sistema StorageGRID perderá a capacidade de ingerir novo conteúdo. Se um alarme for acionado, investigue o motivo da perda do quórum de ADC (por exemplo, pode ser uma falha de rede ou nó de armazenamento) e tome medidas corretivas. Se o problema persistir, entre em Contato com o suporte técnico.
BRDT	Temperatura do chassi do controlador de computação	SSM	Um alarme é acionado se a temperatura do controlador de computação em um dispositivo StorageGRID exceder um limite nominal. Verifique os componentes do hardware e problemas ambientais quanto a condições de sobreaquecimento. Se necessário, substituir o órgão.

Código	Nome	Serviço	Ação recomendada
BTOF	Desvio	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Um alarme é acionado se o tempo de serviço (segundos) diferir significativamente do tempo do sistema operacional. Em condições normais, o serviço deve ressincronizar-se. Se o tempo de serviço se afastar demasiado do tempo do sistema operativo, as operações do sistema podem ser afetadas. Confirme se a fonte de hora do sistema StorageGRID está correta. Se o problema persistir, entre em Contato com o suporte técnico.
BTSE	Estado do relógio	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Um alarme é acionado se a hora do serviço não for sincronizada com a hora rastreada pelo sistema operacional. Em condições normais, o serviço deve ressincronizar-se. Se o tempo se desviar muito longe do tempo do sistema operacional, as operações do sistema podem ser afetadas. Confirme se a fonte de hora do sistema StorageGRID está correta. Se o problema persistir, entre em Contato com o suporte técnico.
CAHP	Porcentagem de uso do Java Heap	DDS	Um alarme é acionado se o Java não conseguir executar a coleta de lixo a uma taxa que permita espaço de heap suficiente para o sistema funcionar corretamente. Um alarme pode indicar uma carga de trabalho do usuário que excede os recursos disponíveis no sistema para o armazenamento de metadados DDS. Verifique a atividade do ILM no painel ou selecione **SUPPORT** > **Tools** > **Grid topology** e, em seguida, selecione ***site*** > ***grid node*** > **DDS** > **Resources** > **Overview** > **Main**. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
CASA	Estado do armazenamento de dados	DDS	Um alarme é acionado se o armazenamento de metadados do Cassandra ficar indisponível. Verifique o status de Cassandra: 1. No nó de armazenamento, faça login como administrador e `su` faça root usando a senha listada no arquivo Passwords.txt. 2. Introduza: `service cassandra status` 3. Se o Cassandra não estiver em execução, reinicie-o: `service cassandra restart` Esse alarme também pode indicar que o armazenamento de metadados (banco de dados Cassandra) para um nó de armazenamento requer reconstrução. Consulte informações sobre como solucionar problemas do alarme Serviços: Status - Cassandra (SVST) no "Solucionar problemas de metadados". Se o problema persistir, entre em Contato com o suporte técnico.
CASO	Estado do armazenamento de dados	DDS	Este alarme é acionado durante a instalação ou expansão para indicar que um novo armazenamento de dados está a aderir à grelha.
CCNA	Hardware de computação	SSM	Esse alarme é acionado se o status do hardware do controlador de computação em um dispositivo StorageGRID precisar de atenção.

Código	Nome	Serviço	Ação recomendada
CDLP	Espaço usado (porcentagem)	DDS	Este alarme é acionado quando o espaço efetivo de metadados (CEMS) atinge 70% cheio (alarme menor), 90% cheio (alarme principal) e 100% cheio (alarme crítico). Se este alarme atingir o limite de 90%, é apresentado um aviso no painel de instrumentos do Gestor de grelhas. Você deve executar um procedimento de expansão para adicionar novos nós de storage o mais rápido possível. "Expanda uma grade"Consulte . Se esse alarme atingir o limite de 100%, você deve parar de ingerir objetos e adicionar nós de storage imediatamente. O Cassandra requer uma certa quantidade de espaço para realizar operações essenciais, como compactação e reparo. Essas operações serão impactadas se os metadados de objetos usarem mais de 100% do espaço permitido. Resultados indesejáveis podem ocorrer. **Nota**: Entre em Contato com o suporte técnico se você não conseguir adicionar nós de storage. Após a adição de novos nós de storage, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de storage e o alarme é apagado. Consulte também informações sobre como solucionar problemas do alerta de armazenamento de metadados baixos no "Solucionar problemas de metadados". Se o problema persistir, entre em Contato com o suporte técnico.
CMNA	Estado CMN	CMN	Se o valor do Status do CMN for erro, selecione **SUPPORT** > **Tools** > **Grid topoly** e, em seguida, selecione ***site*** > ***grid node*** > **CMN** > **Overview** > **Main** e **CMN** > **Alarmes** > **Main** para determinar a causa do erro e solucionar o problema. Um alarme é acionado e o valor de Status do CMN é no Online CMN durante uma atualização de hardware do nó Admin primário quando as CMNs são comutadas (o valor do estado antigo do CMN é Standby e o novo é Online). Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
CPRC	Capacidade restante	NMS	Um alarme é acionado se a capacidade restante (número de conexões disponíveis que podem ser abertas para o banco de dados NMS) ficar abaixo da gravidade do alarme configurada. Se um alarme for acionado, contacte a assistência técnica.
CPSA	Fonte de Alimentação A do controlador de computação	SSM	Um alarme é acionado se houver um problema com a fonte de Alimentação A no controlador de computação para um dispositivo StorageGRID. Se necessário, substituir o órgão.
CPSB	Fonte de alimentação B do controlador de computação	SSM	Um alarme é acionado se houver um problema com a fonte de alimentação B no controlador de computação para um dispositivo StorageGRID. Se necessário, substituir o órgão.
CPUT	Temperatura da CPU do controlador de computação	SSM	Um alarme é acionado se a temperatura da CPU no controlador de computação em um dispositivo StorageGRID exceder um limite nominal. Se o nó de armazenamento for um dispositivo StorageGRID, o sistema StorageGRID indica que o controlador precisa de atenção. Verifique os componentes de hardware e problemas de ambiente quanto a condições de sobreaquecimento. Se necessário, substituir o órgão.
DNST	Estado DNS	SSM	Após a conclusão da instalação, um alarme DNST é acionado no serviço SSM. Depois que o DNS é configurado e as novas informações do servidor atingem todos os nós da grade, o alarme é cancelado.

Código	Nome	Serviço	Ação recomendada
ECCD	Fragmentos corrompidos detetados	LDR	Um alarme é acionado quando o processo de verificação em segundo plano deteta um fragmento corrompido codificado de apagamento. Se um fragmento corrompido for detetado, uma tentativa é feita para reconstruir o fragmento. Redefina os fragmentos corrompidos detetados e copie os atributos perdidos para zero e monitorize-os para ver se as contagens aumentam novamente. Se as contagens aumentarem, pode haver um problema com o armazenamento subjacente do nó de armazenamento. Uma cópia de dados de objeto codificados por apagamento não é considerada ausente até que o número de fragmentos perdidos ou corrompidos viole a tolerância de falhas do código de apagamento; portanto, é possível ter um fragmento corrompido e ainda ser capaz de recuperar o objeto. Se o problema persistir, entre em Contato com o suporte técnico.
ECST	Estado de verificação	LDR	Este alarme indica o estado atual do processo de verificação em segundo plano para dados de objetos codificados por apagamento neste nó de armazenamento. Um alarme principal é acionado se houver um erro no processo de verificação em segundo plano.
FOPN	Abra descritores de arquivo	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	FOPN pode tornar-se grande durante a atividade de pico. Se não diminuir durante períodos de atividade lenta, entre em Contato com o suporte técnico.
HSTE	Estado HTTP	ERRO	Consulte ações recomendadas para HSTU.

Código	Nome	Serviço	Ação recomendada
HSTU	Estado HTTP	ERRO	HSTE e HSTU estão relacionados a HTTP para todo o tráfego LDR, incluindo S3, Swift, e outro tráfego StorageGRID interno. Um alarme indica que ocorreu uma das seguintes situações: • O HTTP foi colocado offline manualmente. • O atributo Auto-Start HTTP foi desativado. • O serviço LDR está a encerrar. O atributo Auto-Start HTTP é ativado por padrão. Se essa configuração for alterada, o HTTP poderá permanecer offline após uma reinicialização. Se necessário, aguarde que o serviço LDR seja reiniciado. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Storage Node*** > **LDR** > **Configuration**. Se o HTTP estiver offline, coloque-o online. Verifique se o atributo Auto-Start HTTP está ativado. Se o HTTP permanecer offline, entre em Contato com o suporte técnico.
HTAS	Auto-Iniciar HTTP	LDR	Especifica se os serviços HTTP devem ser iniciados automaticamente na inicialização. Esta é uma opção de configuração especificada pelo usuário.
IRSU	Estado de replicação de entrada	BLDR, BARC	Um alarme indica que a replicação de entrada foi desativada. Confirme as configurações: Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**.

Código	Nome	Serviço	Ação recomendada
LATA	Latência média	NMS	Verifique se há problemas de conetividade. Verifique a atividade do sistema para confirmar que existe um aumento na atividade do sistema. Um aumento na atividade do sistema resultará em um aumento para atribuir a atividade de dados. Essa atividade aumentada resultará em um atraso no processamento de dados de atributos. Esta pode ser uma atividade normal do sistema e irá diminuir. Verifique se existem vários alarmes. Um aumento nos tempos médios de latência pode ser indicado por um número excessivo de alarmes acionados. Se o problema persistir, entre em Contato com o suporte técnico.
LDRE	Estado LDR	LDR	Se o valor do Estado LDR for Standby (em espera), continue a monitorizar a situação e, se o problema persistir, contacte o suporte técnico. Se o valor de LDR State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
PERDIDO	Objetos perdidos	DDS, LDR	Acionado quando o sistema StorageGRID não consegue recuperar uma cópia do objeto solicitado de qualquer lugar do sistema. Antes de um alarme PERDIDO (objetos perdidos) ser acionado, o sistema tenta recuperar e substituir um objeto em falta de outro local do sistema. Objetos perdidos representam uma perda de dados. O atributo objetos perdidos é incrementado sempre que o número de locais para um objeto cai para zero sem o serviço DDS propositadamente purgando o conteúdo para satisfazer a política ILM. Investigue imediatamente os alarmes PERDIDOS (LOST Object). Se o problema persistir, entre em Contato com o suporte técnico. "Solucionar problemas de dados de objetos perdidos e ausentes"

Código	Nome	Serviço	Ação recomendada
MCEP	Validade do certificado de Interface de Gestão	CMN	Acionado quando o certificado usado para acessar a interface de gerenciamento está prestes a expirar. 1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates**. 2. Na guia **Global**, selecione **certificado de interface de gerenciamento**. 3. "Carregue um novo certificado de interface de gerenciamento."
MINQ	Notificações de e-mail na fila	NMS	Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta. "Configurar as definições do servidor de correio eletrónico para alarmes (sistema legado)"
MIN	Estado das notificações por e-mail	BNMS	Um alarme menor é acionado se o serviço NMS não conseguir se conetar ao servidor de e-mail. Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta. "Configurar as definições do servidor de correio eletrónico para alarmes (sistema legado)"
SAUDADES	Estado do motor da interface NMS	BNMS	Um alarme é acionado se o mecanismo de interface NMS no Admin Node que reúne e gera conteúdo da interface for desconetado do sistema. Verifique o Gerenciador do servidor para determinar se o aplicativo individual do servidor está inativo.
NANG	Configuração de negociação automática de rede	SSM	Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede. Uma definição incorreta pode ter um impactos grave no desempenho do sistema.
NDUP	Configuração Duplex de rede	SSM	Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede. Uma definição incorreta pode ter um impactos grave no desempenho do sistema.

Código	Nome	Serviço	Ação recomendada
NLNK	Detecção de ligação de rede	SSM	Verifique as conexões do cabo de rede na porta e no switch. Verifique as configurações do roteador, do switch e do adaptador de rede. Reinicie o servidor. Se o problema persistir, entre em Contato com o suporte técnico.
NRER	Receber erros	SSM	As seguintes causas podem ser os alarmes NRER: • Correção de erro de avanço (FEC) não corresponde • Incompatibilidade da MTU da porta do switch e da NIC • Altas taxas de erro de link • Buffer de anel NIC excedido Consulte as informações sobre como solucionar problemas do alarme Network Receive Error (NRER) em "Solucionar problemas de rede, hardware e plataforma".
NRLY	Relés de auditoria disponíveis	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se os relés de auditoria não estiverem conetados aos serviços ADC, os eventos de auditoria não poderão ser relatados. Eles estão em fila de espera e indisponíveis para os usuários até que a conexão seja restaurada. Restaure a conetividade a um serviço ADC o mais rápido possível. Se o problema persistir, entre em Contato com o suporte técnico.
NSCA	Estado NMS	NMS	Se o valor de Status do NMS for DB Connectivity Error (erro de conetividade de banco de dados), reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.
NSCE	Estado NMS	NMS	Se o valor do estado NMS for Standby (espera), continue a monitorização e, se o problema persistir, contacte o suporte técnico. Se o valor de Estado NMS for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
VELOCIDADE MÁXIMA	Velocidade	SSM	Isso pode ser causado por problemas de conetividade de rede ou compatibilidade de driver. Se o problema persistir, entre em Contato com o suporte técnico.
NTBR	Livre Tablespace	NMS	Se um alarme for acionado, verifique a rapidez com que a utilização da base de dados foi alterada. Uma queda súbita (ao contrário de uma mudança gradual ao longo do tempo) indica uma condição de erro. Se o problema persistir, entre em Contato com o suporte técnico. Ajustar o limite de alarme permite que você gerencie proativamente quando o armazenamento adicional precisa ser alocado. Se o espaço disponível atingir um limite baixo (consulte o limiar de alarme), contacte o suporte técnico para alterar a alocação da base de dados.
NTER	Transmitir erros	SSM	Esses erros podem ser apagados sem serem reiniciados manualmente. Se eles não limparem, verifique o hardware de rede. Verifique se o hardware e o driver do adaptador estão corretamente instalados e configurados para funcionar com seus roteadores e switches de rede. Quando o problema subjacente for resolvido, reinicie o contador. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**, selecione **Reset Transmit Error Count** e clique em **Apply Changes**.
NTFQ	Desvio de frequência NTP	SSM	Se o desvio de frequência exceder o limite configurado, é provável que haja um problema de hardware com o relógio local. Se o problema persistir, contacte o suporte técnico para agendar uma substituição.
NTLK	Bloqueio NTP	SSM	Se o daemon NTP não estiver bloqueado para uma fonte de tempo externa, verifique a conetividade de rede com as fontes de tempo externas designadas, sua disponibilidade e sua estabilidade.
NTOF	Desvio horário NTP	SSM	Se o desvio de tempo exceder o limite configurado, é provável que haja um problema de hardware com o oscilador do relógio local. Se o problema persistir, contacte o suporte técnico para agendar uma substituição.

Código	Nome	Serviço	Ação recomendada
NTSJ	Jitter de fonte de tempo escolhido	SSM	Este valor indica a confiabilidade e estabilidade da fonte de tempo que o NTP no servidor local está usando como referência. Se um alarme for acionado, pode ser uma indicação de que o oscilador da fonte de tempo está com defeito ou que há um problema com o link WAN para a fonte de tempo.
NTSU	Estado NTP	SSM	Se o valor do Status NTP não estiver em execução, entre em Contato com o suporte técnico.
OPST	Estado geral da alimentação	SSM	Um alarme é acionado se a alimentação de um aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Verifique o estado da fonte de Alimentação A ou B para determinar qual fonte de alimentação está a funcionar de forma anormal. Se necessário, substitua a fonte de alimentação.
OQRT	Objetos em quarentena	LDR	Depois que os objetos são restaurados automaticamente pelo sistema StorageGRID, os objetos em quarentena podem ser removidos do diretório de quarentena. 1. Selecione **SUPPORT** > **Tools** > **Grid topology**. 2. Selecione **site** > **nó de armazenamento** > **LDR** > **Verificação** > **Configuração** > **Principal**. 3. Selecione **Excluir objetos em quarentena**. 4. Clique em **aplicar alterações**. Os objetos em quarentena são removidos e a contagem é redefinida para zero.
ORSU	Estado replicação saída	BLDR, BARC	Um alarme indica que a replicação de saída não é possível: O armazenamento está em um estado em que os objetos não podem ser recuperados. Um alarme é acionado se a replicação de saída for desativada manualmente. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**. Um alarme é acionado se o serviço LDR não estiver disponível para replicação. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Storage**.

Código	Nome	Serviço	Ação recomendada
OSLF	Status do compartimento	SSM	Um alarme é acionado se o status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento for degradado. Os componentes da prateleira de armazenamento incluem IOMs, ventiladores, fontes de alimentação e gavetas de unidade.se este alarme for acionado, consulte as instruções de manutenção do seu aparelho.
PMEM	Utilização da memória de serviço (percentagem)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Pode ter um valor de mais de Y% de RAM, onde Y representa a porcentagem de memória que está sendo usada pelo servidor. Valores abaixo de 80% são normais. Mais de 90% é considerado um problema. Se o uso de memória for alto para um único serviço, monitore a situação e investigue. Se o problema persistir, entre em Contato com o suporte técnico.
PSAS	Estado da fonte de alimentação A.	SSM	Um alarme é acionado se a fonte de Alimentação A num aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Se necessário, substitua a fonte de alimentação A.
PSB	Estado da fonte de alimentação B.	SSM	Um alarme é acionado se a fonte de alimentação B num aparelho StorageGRID se desviar da tensão de funcionamento recomendada. Se necessário, substitua a fonte de alimentação B..
RDTE	Estado do Tivoli Storage Manager	BARC	Disponível apenas para nós de arquivamento com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do estado do Tivoli Storage Manager estiver offline, verifique o status do Tivoli Storage Manager e resolva quaisquer problemas. Coloque o componente novamente online. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **ARC** > **Target** > **Configuration** > **Main**, selecione **Tivoli Storage Manager State** > **Online** e clique em **Apply Changes**.

Código	Nome	Serviço	Ação recomendada
RDTU	Status do Tivoli Storage Manager	BARC	Disponível apenas para nós de arquivamento com um tipo de destino do Tivoli Storage Manager (TSM). Se o valor do status do Gerenciador de armazenamento Tivoli for erro de configuração e o nó de arquivo tiver sido adicionado ao sistema StorageGRID, verifique se o servidor de middleware TSM está configurado corretamente. Se o valor do status do Gerenciador de armazenamento Tivoli for falha de conexão ou falha de conexão, tente novamente, verifique a configuração de rede no servidor middleware TSM e a conexão de rede entre o servidor de middleware TSM e o sistema StorageGRID. Se o valor do status do Gerenciador de armazenamento Tivoli for Falha de autenticação ou Falha de autenticação, reconetando, o sistema StorageGRID poderá se conetar ao servidor middleware TSM, mas não poderá autenticar a conexão. Verifique se o servidor de middleware TSM está configurado com o usuário, senha e permissões corretos e reinicie o serviço. Se o valor do status do Tivoli Storage Manager for Falha da sessão, uma sessão estabelecida foi perdida inesperadamente. Verifique a conexão de rede entre o servidor middleware TSM e o sistema StorageGRID. Verifique se há erros no servidor middleware. Se o valor do status do Tivoli Storage Manager for erro desconhecido, entre em Contato com o suporte técnico.
RIRF	Replicações de entrada — falhou	BLDR, BARC	Um alarme Inbound replicações — Falha pode ocorrer durante períodos de alta carga ou interrupções temporárias da rede. Após a redução da atividade do sistema, este alarme deve ser apagado. Se a contagem de replicações falhadas continuar a aumentar, procure problemas de rede e verifique se os serviços LDR e ARC de origem e destino estão online e disponíveis. Para repor a contagem, selecione **support** > **Tools** > **Grid topoly** e, em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. Selecione **Redefinir contagem de falhas de replicação de entrada** e clique em **aplicar alterações**.

Código	Nome	Serviço	Ação recomendada
RIRQ	Replicações de entrada — na fila	BLDR, BARC	Os alarmes podem ocorrer durante períodos de alta carga ou interrupção temporária da rede. Após a redução da atividade do sistema, este alarme deve ser apagado. Se a contagem de repetições em fila continuar a aumentar, procure problemas de rede e verifique se os serviços LDR e ARC de origem e destino estão online e disponíveis.
RORQ	Repetições de saída — em fila	BLDR, BARC	A fila de replicação de saída contém dados de objeto que estão sendo copiados para satisfazer as regras e objetos ILM solicitados pelos clientes. Um alarme pode ocorrer como resultado de uma sobrecarga do sistema. Aguarde para ver se o alarme é apagado quando a atividade do sistema diminui. Se o alarme voltar a ocorrer, adicione capacidade adicionando nós de storage.
SAVP	Espaço utilizável total (percentagem)	LDR	Se o espaço utilizável atingir um limite baixo, as opções incluem a expansão do sistema StorageGRID ou a movimentação de dados de objetos para arquivamento por meio de um nó de arquivamento.
SCAS	Estado	CMN	Se o valor de Status para a tarefa de grade ativa for erro, procure a mensagem de tarefa de grade. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Overview** > **Main**. A mensagem de tarefa de grade exibe informações sobre o erro (por exemplo, "verificação falhou no nó 12130011"). Depois de investigar e corrigir o problema, reinicie a tarefa de grade. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **Main** e selecione **Actions** > **Run**. Se o valor de Status para uma tarefa de grade que está sendo interrompida for erro, tente terminar novamente a tarefa de grade. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
SCEP	Validade do certificado de Endpoints do Serviço de API de armazenamento	CMN	Acionado quando o certificado usado para acessar endpoints de API de armazenamento está prestes a expirar. 1. Selecione **CONFIGURATION** > **Security** > **Certificates**. 2. Na guia **Global**, selecione **S3 e Swift API certificate**. 3. "Faça upload de um novo certificado API S3 e Swift."
SCHR	Estado	CMN	Se o valor de Status para a tarefa de grade histórica for abortado, investigue o motivo e execute a tarefa novamente, se necessário. Se o problema persistir, entre em Contato com o suporte técnico.
SCSA	Controlador de armazenamento A	SSM	Um alarme é acionado se houver um problema com o controlador de armazenamento A em um dispositivo StorageGRID. Se necessário, substituir o órgão.
SCSB	Controlador de armazenamento B	SSM	Um alarme é acionado se houver um problema com o controlador de armazenamento B em um dispositivo StorageGRID. Se necessário, substituir o órgão. Alguns modelos de aparelhos não têm um controlador de armazenamento B..
SHLH	Saúde	LDR	Se o valor de integridade para um armazenamento de objetos for erro, verifique e corrija: • problemas com o volume a ser montado • erros do sistema de arquivos

Código	Nome	Serviço	Ação recomendada
SLSA	Média de carga da CPU	SSM	Quanto maior for o valor, mais ocupado o sistema. Se a média de carga da CPU persistir em um valor alto, o número de transações no sistema deve ser investigado para determinar se isso se deve a uma carga pesada no momento. Veja um gráfico da média de carga da CPU: Selecione **SUPPORT** > **Tools** > **Grid topoly**. Em seguida, selecione ***site*** > ***grid node*** > **SSM** > **Resources** > **Reports** > **Charts**. Se a carga no sistema não for pesada e o problema persistir, contacte a assistência técnica.
SMST	Estado do monitor de registo	SSM	Se o valor do Estado do Monitor de Registos não estiver ligado durante um período de tempo persistente, contacte o suporte técnico.
SMTT	Total de eventos	SSM	Se o valor de Eventos totais for maior que zero, verifique se existem eventos conhecidos (como falhas de rede) que podem ser a causa. A menos que esses erros tenham sido apagados (ou seja, a contagem foi redefinida para 0), os alarmes de Total de Eventos podem ser acionados. Quando um problema for resolvido, reponha o contador para apagar o alarme. Selecione **NÓS** > ***site*** > ***grid node*** > **Eventos** > **Redefinir contagens de eventos**. Para redefinir contagens de eventos, você deve ter a permissão de configuração de página de topologia de Grade. Se o valor de Total de Eventos for zero ou o número aumentar e o problema persistir, contacte o suporte técnico.
SNST	Estado	CMN	Um alarme indica que há um problema ao armazenar os pacotes de tarefas da grade. Se o valor de Status for erro de Checkpoint ou Quórum não atingido, confirme que a maioria dos serviços ADC está conetada ao sistema StorageGRID (50% mais um) e aguarde alguns minutos. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
SOSS	Estado do sistema operativo de armazenamento	SSM	Um alarme é acionado se o sistema operacional SANtricity indicar que há um problema de "necessidade de atenção" com um componente em um dispositivo StorageGRID. Selecione **NODES**. Em seguida, selecione **nó de armazenamento do dispositivo** > **hardware**. Role para baixo para ver o status de cada componente. No SANtricity os, verifique outros componentes do dispositivo para isolar o problema.
SSMA	Estado SSM	SSM	Se o valor de Status SSM for erro, selecione **SUPPORT** > **Tools** > **Grid topoly** e, em seguida, selecione ***site*** > ***grid node*** > **SSM** > **Overview** > **Main** e **SSM** > **Overview** > **Alarmes** para determinar a causa do alarme. Se o problema persistir, entre em Contato com o suporte técnico.
SSME	Estado SSM	SSM	Se o valor do estado SSM for Standby (em espera), continue a monitorização e, se o problema persistir, contacte a assistência técnica. Se o valor do estado SSM for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
SSTS	Estado de armazenamento	ERRO	Se o valor do Status do armazenamento for espaço utilizável insuficiente, não haverá mais armazenamento disponível no nó de armazenamento e os ingeries de dados serão redirecionados para outro nó de armazenamento disponível. As solicitações de recuperação podem continuar a ser entregues a partir deste nó de grade. Armazenamento adicional deve ser adicionado. Ele não está impactando a funcionalidade do usuário final, mas o alarme persiste até que o armazenamento adicional seja adicionado. Se o valor de Status do armazenamento for volume(s) indisponível(s), uma parte do armazenamento não estará disponível. O armazenamento e a recuperação destes volumes não são possíveis. Verifique o volume's Health (Saúde do volume) para obter mais informações: Selecione **SUPPORT** > **Tools** (SUPORTE* > Ferramentas* > **Grid topology**). Em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. O volume's Health (Saúde do volume) está listado em Object Stores. Se o valor do Status do armazenamento for erro, entre em Contato com o suporte técnico. "Solucione o problema do alarme de Status de armazenamento (SSTS)"

Código	Nome	Serviço	Ação recomendada
SVST	Estado	SSM	Este alarme é apagado quando outros alarmes relacionados a um serviço que não está em execução são resolvidos. Acompanhe os alarmes de serviço de origem para restaurar a operação. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **SSM** > **Serviços** > **Visão geral** > **Principal**. Quando o status de um serviço é mostrado como não em execução, seu estado é administrativamente inativo. O status do serviço pode ser listado como não em execução pelos seguintes motivos: • O serviço foi interrompido manualmente (`/etc/init.d/<service\> stop`). • Há um problema com o banco de dados MySQL e o Server Manager desliga o serviço MI. • Um nó de grade foi adicionado, mas não iniciado. • Durante a instalação, um nó de grade ainda não se conetou ao nó Admin. Se um serviço estiver listado como não em execução, reinicie o serviço (`/etc/init.d/<service\> restart`). Esse alarme também pode indicar que o armazenamento de metadados (banco de dados Cassandra) para um nó de armazenamento requer reconstrução. Se o problema persistir, entre em Contato com o suporte técnico. "Solucionar problemas do alarme Serviços: Status - Cassandra (SVST)"
TMEM	Memória instalada	SSM	Os nós executados com menos de 24 GiB de memória instalada podem levar a problemas de performance e instabilidade do sistema. A quantidade de memória instalada no sistema deve ser aumentada para pelo menos 24 GiB.
TPOP	Operações pendentes	ADC	Uma fila de mensagens pode indicar que o serviço ADC está sobrecarregado. Poucos serviços ADC podem ser conetados ao sistema StorageGRID. Em uma grande implantação, o serviço ADC pode exigir a adição de recursos computacionais, ou o sistema pode exigir serviços ADC adicionais.

Código	Nome	Serviço	Ação recomendada
UMEM	Memória disponível	SSM	Se a RAM disponível ficar baixa, determine se este é um problema de hardware ou software. Se não for um problema de hardware ou se a memória disponível for inferior a 50 MB (o limite de alarme predefinido), contacte o suporte técnico.
VMFI	Entradas disponíveis	SSM	Esta é uma indicação de que é necessário um armazenamento adicional. Entre em Contato com o suporte técnico.
VMFR	Espaço disponível	SSM	Se o valor de espaço disponível ficar muito baixo (consulte limiares de alarme), ele precisa ser investigado se há arquivos de log crescendo fora de proporção, ou objetos ocupando muito espaço em disco (veja limiares de alarme) que precisam ser reduzidos ou excluídos. Se o problema persistir, entre em Contato com o suporte técnico.
VMST	Estado	SSM	Um alarme é acionado se o valor de Status para o volume montado for desconhecido. Um valor desconhecido ou Offline pode indicar que o volume não pode ser montado ou acessado devido a um problema com o dispositivo de armazenamento subjacente.
VPRI	Prioridade de verificação	BLDR, BARC	Por padrão, o valor da prioridade de verificação é adaptável. Se a prioridade de verificação estiver definida como alta, um alarme é acionado porque a verificação do armazenamento pode retardar as operações normais do serviço.
VSTU	Estado Verificação Objeto	ERRO	Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Verifique se existem sinais de erros no sistema operativo ou no sistema de ficheiros. Se o valor do Status de Verificação de Objeto for erro desconhecido, ele geralmente indica um problema de hardware ou sistema de arquivos de baixo nível (erro de e/S) que impede que a tarefa de Verificação de armazenamento acesse conteúdo armazenado. Entre em Contato com o suporte técnico.

Código	Nome	Serviço	Ação recomendada
XAMS	Repositórios de auditoria inalcançáveis	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Verifique a conetividade de rede ao servidor que hospeda o nó Admin. Se o problema persistir, entre em Contato com o suporte técnico.

Referência de ficheiros de registo

Referência de ficheiros de registo: Visão geral

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 para o suporte técnico para ajudar na solução de problemas.

Os logs são categorizados da seguinte forma:

- "Registos do software StorageGRID"
- "Logs de implantação e manutenção"
- "Logs para software de terceiros"
- "Sobre o bycast.log"

> Os detalhes fornecidos para cada tipo de log são apenas para referência. Os registos destinam-se à resolução de problemas avançada por 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 dessas instruções.

Aceder aos registos

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

1. Introduza o seguinte comando: `ssh admin@grid_node_IP`
2. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
3. Digite o seguinte comando para mudar para root: `su -`
4. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Categorias de ficheiros de registo

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.

Localização do arquivo	Descrição
base-os-logs	Informações básicas do sistema operacional, incluindo versões de imagem StorageGRID.
pacotes	Informações de configuração global (pacotes).
cassandra	Informações do banco de dados Cassandra e Registros de reparo do Reaper.
ce	Informações de VCSs sobre o nó atual e as informações de grupo EC por ID de perfil.
grelha	Logs gerais de grade incluindo debug (`bycast.log`) e `servermanager` logs.
grid.xml	Arquivo de configuração de grade compartilhado em todos os nós.
grupos	A alta disponibilidade agrupa métricas e logs.
instale	`Gdu-server` e instalar logs.
lumberjack.log	Depurar mensagens relacionadas à coleção de logs.
Lambda-árbitro	Logs relacionados à solicitação de proxy S3 Select.
Métricas	Logs de serviço para Grafana, Jaeger, nó exportador e Prometheus.
miscd	Registos de acesso e erro incorretos.
mysql	A configuração do banco de dados MariaDB e logs relacionados.
rede	Logs gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos e logs de configuração de federação de grade e balanceador de carga. Também inclui logs de tráfego do Grid Manager e do Tenant Manager.
nginx-gw	Arquivos e logs de configuração de federação de grade e balanceador de carga.
ntp	Ficheiro de configuração NTP e registos.
so	Arquivo de estado de nó e grade, incluindo serviços `pid`.
outros	Arquivos de log sob `/var/local/log` que não são coletados em outras pastas.
perf	Informações de desempenho para CPU, rede e e/S de disco

Localização do arquivo	Descrição
prometheus-data	Métricas atuais do Prometheus, se a coleção de logs incluir dados do Prometheus.
provisionamento	Logs relacionados ao processo de provisionamento de grade.
jangada	Registros do cluster de jangada usados em serviços de plataforma.
ssh	Logs relacionados à configuração e serviço SSH.
snmp	Configuração do agente SNMP e listas de permissão/negação de alarme usadas para enviar notificações SNMP.
sockets-dados	Dados de sockets para depuração de rede.
system-commands.txt	Saída de comandos StorageGRID Container. Contém informações do sistema, como utilização de rede e disco.

Registos do software StorageGRID

Você pode usar logs do StorageGRID para solucionar problemas.

Se pretender enviar os seus registos para um servidor syslog externo ou alterar o destino das informações de auditoria, como a `bycast.log` e `nms.log`, "Configurar mensagens de auditoria e destinos de log"consulte .

Registos gerais do StorageGRID

Nome do ficheiro	Notas	Encontrado em
/var/local/log/bycast.log	O arquivo primário de solução de problemas do StorageGRID. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos os nós
/var/local/log/bycast-err.log	Contém um subconjunto de `bycast.log` (mensagens com ERRO de gravidade e CRÍTICO). Mensagens CRÍTICAS também são exibidas no sistema. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos os nós

Nome do ficheiro	Notas	Encontrado em
/var/local/core/	Contém quaisquer arquivos de despejo de núcleo criados se o programa terminar anormalmente. As possíveis causas incluem falhas de asserção, violações ou tempos limite de thread. **Nota**: O arquivo `/var/local/core/kexec_cmd` geralmente existe em nós de appliance e não indica um erro.	Todos os nós

Registos relacionados com cifras

Nome do ficheiro	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 nginx-gw (e recarregamento de serviços nginx-gw).	Nós de administrador e gateway
/var/local/log/update-cipher-configurations.log	Contém logs relacionados à configuração de políticas TLS e SSH.	Todos os nós

Logs de federação de grade

Nome do ficheiro	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

Registos NMS

Nome do ficheiro	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, processamento de alarmes, 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 ao atributo downsampling feito 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 às 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 Server Manager

Nome do ficheiro	Notas	Encontrado em
/var/local/log/servermanager.log	Ficheiro de registo para a aplicação Gestor de servidor em execução no servidor.	Todos os nós
/Var/local/log/GridstatBackend.errlog	Ficheiro de registo para a aplicação de back-end GUI do Gestor de servidor.	Todos os nós
/var/local/log/gridstat.errlog	Ficheiro de registo para a GUI do Gestor de servidor.	Todos os nós

Registos de serviços do StorageGRID

Nome do ficheiro	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de storage 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 storage executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/arc.errlog		Nós de arquivamento
/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 nodetool for interrompida.	Nós de storage
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que executa reparos dos dados no banco de dados Cassandra.	Nós de storage
/var/local/log/cassandra-reaper.errlog	Informações de erro para o serviço Cassandra Reaper.	Nós de storage
/var/local/log/chunk.errlog		Nós de storage
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Esse arquivo de log pode estar presente em sistemas que foram atualizados a partir de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de storage
/var/local/log/cts.errlog	Esse arquivo de log só será criado se o tipo de destino for **Cloud Tiering - Simple Storage Service (S3).**	Nós de arquivamento
/var/local/log/dds.errlog		Nós de storage

Nome do ficheiro	Notas	Encontrado em
/var/local/log/dmv.errlog		Nós de storage
/var/local/log/dynip*	Contém logs relacionados ao serviço dynip, que monitora a grade para alterações dinâmicas de IP e atualiza a configuração local.	Todos os nós
/var/local/log/grafana.log	O log associado ao serviço Grafana, que é usado para visualização de métricas no Gerenciador de Grade.	Nós de administração
/var/local/log/hagroups.log	O log associado a grupos de alta disponibilidade.	Nós de administração e nós de gateway
/var/local/log/hagroups_events.log	Controla as alterações de estado, como a transição do backup para O MESTRE ou FALHA.	Nós de administração e nós de gateway
/var/local/log/idnt.errlog		Nós de storage 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 storage executando o serviço ADC
/var/local/log/lambda*	Contém registos para o serviço S3 Select.	Nós de administrador e gateway Apenas alguns nós de Admin e Gateway contêm esse log. Consulte "S3 Selecione requisitos e limitações para os nós de administração e de gateway".
/var/local/log/ldr.errlog		Nós de storage

Nome do ficheiro	Notas	Encontrado em
/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 dos serviços em execução em outros nós.	Todos os nós
/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 falar com serviços em outros nós através de APIs HTTPS.	Todos os nós
/var/local/log/nginx-gw/*.log	Contém logs gerais relacionados ao serviço nginx-gw, incluindo logs de erro e logs para as 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 registos de acesso relacionados com o tráfego de replicação entre redes.	Nós de administração, nós de gateway ou ambos, com base na configuração da federação de grade. Apenas encontrado na grelha de destino para replicação entre grelha.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contém logs de acesso para o serviço Load Balancer, que fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage.	Nós de administração e nós de gateway
/var/local/log/persistence*	Contém logs para o serviço Persistence, que gerencia arquivos no disco raiz que precisam persistir durante uma reinicialização.	Todos os nós
/var/local/log/prometheus.log	Para todos os nós, contém o log de serviço de exportador de nós e o log de serviço de métricas ade-exportador. For Admin node, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós

Nome do ficheiro	Notas	Encontrado em
/var/local/log/raft.log	Contém a saída da biblioteca usada pelo serviço RSM para o protocolo Raft.	Nós de storage com serviço RSM
/var/local/log/rms.errlog	Contém registos para o serviço RSM (Serviço de Máquina de Estado replicado), que é utilizado para serviços de plataforma S3.	Nós de storage com serviço RSM
/var/local/log/ssm.errlog		Todos os nós
/var/local/log/update-s3vs-domains.log	Contém logs relacionados ao processamento de atualizações para a configuração de nomes de domínio hospedados virtuais S3.consulte as instruções para implementar aplicativos cliente S3.	Nós de administrador e gateway
/var/local/log/update-snmp-firewall.*	Contém registos relacionados com as portas de firewall a gerir para SNMP.	Todos os nós
/var/local/log/update-sysl.log	Contém logs relacionados às alterações feitas na configuração do syslog do sistema.	Todos os nós
/var/local/log/update-traffic-classes.log	Contém registos relacionados com alterações na configuração dos classificadores de tráfego.	Nós de administrador e gateway
/var/local/log/update-utcn.log	Contém registos relacionados com o modo rede Cliente não fidedigno neste nó.	Todos os nós

Informações relacionadas

"Sobre o bycast.log"

"USE A API REST DO S3"

Logs de implantação e manutenção

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/install.log	Criado durante a instalação do software. Contém um registo dos eventos de instalação.	Todos os nós

Nome do ficheiro	Notas	Encontrado em
/var/local/log/expansion-progress.log	Criado durante operações de expansão. Contém um Registro dos eventos de expansão.	Nós de storage
/var/local/log/pa-move.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/var/local/log/pa-move-new_pa.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/var/local/log/pa-move-old_pa.log	Criado durante a execução `pa-move.sh` do script.	Nó de administração principal
/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 principal
/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 de software. Contém um registo dos eventos de atualização de software.	Todos os nós

Logs para software de terceiros

Você pode usar os logs de software de terceiros para solucionar problemas.

Categoria	Nome do ficheiro	Notas	Encontrado em
Arquivamento	/var/local/log/dsierror.log	Informações de erro para as APIs do cliente TSM.	Nós de arquivamento
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	Arquivos de log gerados pelo MySQL. `mysql.err` captura erros de banco de dados e eventos, como startups e paradas. `mysql-slow.log` (O log de consulta lenta) captura as instruções SQL que levaram mais de 10 segundos para serem executadas.	Nós de administração

Categoria	Nome do ficheiro	Notas	Encontrado em
Sistema operacional	/var/local/log/messages	Este diretório contém ficheiros de registo para o sistema operativo. Os erros contidos nesses logs também são exibidos no Gerenciador de Grade. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione **topologia** > ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos os nós
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Contém o arquivo de log para mensagens de erro NTP. `/var/lib/ntp/var/log/ntpstats/` O diretório contém estatísticas de tempo NTP. `loopstats` registra informações estatísticas de filtro de loop. `peerstats` registra informações estatísticas de pares.	Todos os nós

Sobre o bycast.log

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

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

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 a ser gerados e armazenados quando um servidor syslog externo é configurado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Rotação de ficheiros para bycast.log

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

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

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

Se um arquivo de log tiver sido compactado, você não deve descompactá-lo para o mesmo local em que foi escrito. A descompressão do arquivo para o mesmo local pode interferir com os 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 a ser gerados e armazenados quando um servidor syslog externo é configurado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Informações relacionadas

"Colete arquivos de log e dados do sistema"

Mensagens em bycast.log

As mensagens em `bycast.log` são escritas pelo ADE (Asynchronous Distributed Environment). ADE é o ambiente de tempo de execução usado pelos serviços de cada nó de 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 mensagens	Valor no exemplo
ID de nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador da mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29,784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUUUUUU)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação do estado do volume 3 falhou com o motivo "TOUT"

Severidades da mensagem em bycast.log

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

Por exemplo:

- **AVISO** — ocorreu um evento que deve ser gravado. A maioria das mensagens de log estão nesse nível.
- **AVISO** — ocorreu uma condição inesperada.
- **ERROR** — ocorreu Um erro importante que afetará as operações.
- **CRÍTICO** — ocorreu uma condição anormal que parou as operações normais. Você deve abordar a condição subjacente imediatamente. Mensagens críticas também são exibidas no Gerenciador de Grade. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione **Site** > **nó** > **SSM** > **Eventos**.

Códigos de erro em `bycast.log`

A maioria das mensagens de erro no `bycast.log` contém 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 é relatado.

Código de erro	Significado
SUCS	Nenhum erro
GERR	Desconhecido
CANC	Cancelado
ABRT	Abortado
SAÍDA	Tempo limite
INVL	Inválido
NFND	Não encontrado
VERS	Versão
CONF	Configuração
FALHA	Falha
ICPL	Incompleto
CONCLUÍDO	Concluído
SUNV	Serviço indisponível

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

Número de erro	Código de erro	Significado
001	EPERM	Operação não permitida
002	ENOENT	Nenhum tal arquivo ou diretório
003	ESRCH	Nenhum tal processo
004	EINTR	Chamada do sistema interrompida
005	EIO	Erro de e/S.
006	ENXIO	Nenhum dispositivo ou endereço
007	E2BIG	Lista de argumentos demasiado longa
008	ENOEXEC	Erro de formato Exec
009	EBADF	Número de ficheiro incorreto
010	ECHILD	Nenhum processo filho
011	EAGAIN	Tente novamente
012	ENOMEM	Sem memória
013	EACCES	Permissão negada
014	EFAULT	Endereço incorreto
015	ENOTBLK	Bloquear dispositivo necessário
016	EBUSY	Dispositivo ou recurso ocupado
017	EEXIST	O ficheiro existe
018	EXDEV	Ligação entre dispositivos
019	ENODEV	Nenhum desses dispositivos
020	ENOTDIR	Não é um diretório
021	EISDIR	É um diretório
022	EINVAL	Argumento inválido

Número de erro	Código de erro	Significado
023	ENFILE	Estouro da tabela de arquivos
024	EMFILE	Demasiados ficheiros abertos
025	ENOTTY	Não é uma máquina de escrever
026	ETXTBSY	Ficheiro de texto ocupado
027	EFBIG	Ficheiro demasiado grande
028	ENOSPC	Nenhum espaço restante no dispositivo
029	ESPIPE	Procura ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Demasiados links
032	EPIPE	Tubo quebrado
033	EDOM	Argumento de matemática fora de domínio do func
034	ERANGE	Resultado matemático não representável
035	EDEADLK	O bloqueio de recursos ocorreria
036	ENAMETOOLONG	Nome do ficheiro demasiado longo
037	ENOLCK	Não existem bloqueios de registo disponíveis
038	ENOSYS	Função não implementada
039	ENOTEMPTY	O diretório não está 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

Número de erro	Código de erro	Significado
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Reposição do nível 3
048	ELNRNG	Número da ligação fora do intervalo
049	EUNATCH	Controlador 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 pedido inválido
057	EBADSLT	Ranhura inválida
058		
059	EBFONT	Formato de arquivo de fonte incorreto
060	ENOSTR	Dispositivo não é um fluxo
061	ENODATA	Nenhum dado disponível
062	ETIME	O temporizador expirou
063	ENOSR	Recursos fora de fluxos
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado
066	EREMOTE	O objeto é remoto

Número de erro	Código de erro	Significado
067	ENOLINK	O link foi cortado
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação no envio
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de Multihop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	EOVERFLOW	Valor demasiado 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 em muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada do sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro no tubo de fluxos

Número de erro	Código de erro	Significado
087	EUSERS	Demasiados utilizadores
088	ENOTSOCK	Funcionamento da tomada sem tomada
089	EDESTADDRREQ	Endereço de destino obrigatório
090	EMSGSIZE	Mensagem demasiado longa
091	EPROTOTYPE	Protocolo tipo errado para socket
092	ENOPROTOOPT	Protocolo não disponível
093	EPROTONOSUPPORT	Protocolo não suportado
094	ESOCKTNOSUPPORT	Tipo de soquete não suportado
095	EOPNOTSUPP	Operação não suportada no terminal de transporte
096	EPFNOSUPPORT	Família de protocolos não suportada
097	EAFNOSUPPORT	Família de endereços não suportada pelo protocolo
098	EADDRINUSE	Endereço já em uso
099	EADDRNOTAVAIL	Não é possível atribuir o endereço solicitado
100	ENETDOWN	A rede está inativa
101	ENETUNREACH	A rede não está acessível
102	ENETRESET	A ligação à rede foi interrompida devido à reposição
103	ECONNABORTED	O software fez com que a conexão terminasse
104	ECONNRESET	Conexão redefinida por ponto
105	ENOBUFS	Nenhum espaço de buffer disponível
106	EISCONN	O terminal de transporte já está ligado
107	ENOTCONN	O terminal de transporte não está ligado

Número de erro	Código de erro	Significado
108	ESHUTDOWN	Não é possível enviar após o encerramento do endpoint de transporte
109	ETOOMANYREFS	Muitas referências: não é possível unir
110	ETIMEDOUT	Tempo de ligação esgotado
111	ECONNREFUSED	Ligação recusada
112	EHOSTDOWN	O host está inativo
113	EHOSTUNREACH	Nenhuma rota para o host
114	EALREADY	Operação já em curso
115	EINPROGRESS	Operação agora em andamento
116		
117	EUCLEAN	Estrutura precisa de limpeza
118	ENOTNAM	Não é um arquivo de tipo chamado XENIX
119	ENAVAIL	Não há semáforos XENIX disponíveis
120	EISNAM	É um arquivo de tipo nomeado
121	EREMOTEIO	Erro de e/S remota
122	EDQUOT	Quota excedida
123	ENOMEDIUM	Nenhum meio encontrado
124	EMEDIUMTYPE	Tipo médio errado
125	ECANCELED	Operação cancelada
126	ENOKEY	Chave necessária não disponível
127	EKEYEXPIRED	A chave expirou
128	EKEYREVOKED	A chave foi revogada

Número de erro	Código de erro	Significado
129	EKEYREJECTED	A chave foi rejeitada pelo serviço de revisão
130	EOWNERDEAD	Para mutexes robustos: O proprietário morreu
131	ENOTRECOVERABLE	Para mutexes robustos: Estado não recuperável

Configurar destinos de mensagens de auditoria e de log

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. O uso de 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 de pacote de mensagens syslog de saída é compatível com RFC 3164.

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

- Logs de auditoria contendo as mensagens de auditoria geradas durante a operação normal do sistema
- Eventos relacionados à segurança, como logins e escalações para o root
- Logs de aplicativos que podem ser solicitados se for necessário abrir um caso de suporte para solucionar um problema encontrado

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 nos nós de administração porque as informações de auditoria são transferidas diretamente dos vários nós de storage para o servidor syslog externo, sem ter que 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 servidor syslog externo.

> 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 saber como configurar um servidor syslog externo, "Configurar mensagens de auditoria e servidor syslog externo"consulte .

Se você pretende 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 padrão da CA de grade será usado.
- **Certificado de cliente**: O certificado de cliente para autenticação para o 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, você também deve usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, você também deve fornecer a senha. Não há benefício significativo de segurança ao usar 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 alcançar uma taxa de transferência necessária, definida em termos de S3 operações por segundo ou bytes por segundo. Por exemplo, você pode ter um requisito de que sua grade lide com 1.000 S3 operações por segundo, ou 2.000 MB por segundo, de inclusões 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 a estimar a taxa e o tamanho médio de mensagens de log de vários tipos que seu servidor syslog externo precisa ser capaz de lidar, expressas em termos das caraterísticas de desempenho conhecidas ou desejadas da grade (S3 operações por segundo).

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

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

Fórmulas de estimativa para logs de auditoria

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações 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, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os valores padrão (todas as categorias definidas como normal, exceto armazenamento, que está 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 S3 operações por segundo, seu servidor syslog externo deve ser dimensionado para suportar 2.000 mensagens syslog por segundo e deve ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de 1,6 MB por segundo.

Se você sabe mais sobre sua carga de trabalho, estimativas mais precisas são possíveis. Para logs de auditoria, as variáveis adicionais mais importantes são a porcentagem de S3 operações que são puts (vs. GETS), e o tamanho médio, em bytes, dos S3 campos a seguir (abreviações de 4 carateres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Vamos usar P para representar a porcentagem de S3 operações que são puts, onde 0 ≤ P ≤ 1 (assim, 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 conta S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm 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, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os padrões (todas as categorias definidas como normal, exceto armazenamento, que está 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 S3 operações por segundo, sua carga de trabalho é de 50% puts, e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1.500 mensagens syslog por segundo e

deve 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 assumem 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 das 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 é provável que isso resulte em uma estimativa excessiva porque as mensagens de auditoria "extra" são, em média, menores do que as mensagens de auditoria padrão.

Condição	Fórmula
Replicação: Níveis de auditoria todos definidos como Debug ou normal	Taxa de log de auditoria: 8 x S3 taxa de operações
Codificação de apagamento: Níveis de auditoria todos definidos como Debug ou normal	Use a mesma fórmula que para as configurações padrão

Fórmulas de estimativa para eventos de segurança

Os eventos de segurança não estão correlacionados com as operações do S3 e normalmente produzem um volume insignificante de logs e dados. Por estas razões, não são fornecidas fórmulas de estimativa.

Fórmulas de estimativa para logs de aplicativos

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de Registros de aplicativos que seu servidor syslog externo precisará lidar com 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 S3 operações por segundo, seu servidor syslog externo deve ser dimensionado para suportar 3.300 Registros 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 sabe mais sobre sua carga de trabalho, estimativas mais precisas são possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. Codificação de apagamento), a porcentagem de operações S3 que são puts (vs. Gets/other) e o tamanho médio, em bytes, dos S3 campos a seguir (abreviações de 4 carateres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.

Código	Campo	Descrição
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Exemplo de estimativas de dimensionamento

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

- Replicação
- Codificação de apagamento

Se você usar a replicação para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde 0 ≤ P ≤ 1 (assim, 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 S3 nomes de conta, S3 bucket e S3 key. Suponha que o nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm 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, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de lidar com 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 é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1800 Registros 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 apagamento para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde 0 ≤ P ≤ 1 (assim, 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 S3 nomes de conta, S3 bucket e S3 key. Suponha que o

nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm 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, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de lidar com 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
```

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 2.250 Registros de aplicativos por segundo e deve 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

Pode configurar várias definições relacionadas com mensagens de auditoria. Você pode ajustar o número de mensagens de auditoria registradas; definir quaisquer cabeçalhos de solicitação HTTP que você deseja incluir em mensagens de auditoria de leitura e gravação de cliente; configurar um servidor syslog externo; e especificar onde os logs de auditoria, logs de eventos de segurança e logs de software do StorageGRID são enviados.

Mensagens de auditoria e logs 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 a atividade e os eventos do sistema.

Opcionalmente, você pode configurar um servidor syslog externo para salvar informações de auditoria remotamente. O uso de um servidor externo minimiza o impactos 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. "Considerações para servidor syslog externo"Consulte para obter detalhes.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Se você planeja configurar um servidor syslog externo, revisou o "considerações para usar um servidor syslog externo" e garantiu que o servidor tem 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 terá a CA de servidor e os certificados de cliente necessários e a chave privada do cliente.

Alterar os 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	Predefinição	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"
Armazenamento	Erro	"Mensagens de auditoria de armazenamento de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gerenciamento"
O cliente lê	Normal	"O cliente lê mensagens de auditoria"
O cliente escreve	Normal	"O cliente escreve mensagens de auditoria"
ILM	Normal	"Mensagens de auditoria ILM"
Replicação entre grade	Erro	"CGRR: Solicitação de replicação de Grade cruzada"

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 **CONFIGURATION** > **Monitoring** > **Audit and syslog Server**.
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	As mensagens transacionais padrão são registradas - as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível comporta-se da mesma forma que o nível normal de auditoria.

As mensagens incluídas para qualquer nível particular 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 de cliente para seus aplicativos S3, altere opcionalmente a configuração **leitura de cliente** para **erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria.

3. Selecione **Guardar**.

   Um banner verde indica que sua configuração foi salva.

Definir cabeçalhos de solicitação HTTP

Opcionalmente, você pode definir qualquer cabeçalho de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação de cliente. Estes cabeçalhos de protocolo aplicam-se apenas às solicitações S3 e Swift.

Passos

1. Na seção **cabeçalhos de 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 carateres. 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 sob o campo HTRH.

   > Os cabeçalhos de solicitação de protocolo de auditoria são registrados somente se o nível de auditoria para **leitura do cliente** ou **gravações do cliente** não for **desativado**.

3. Selecione **Guardar**

   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 grade.

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

> Se as opções de configuração disponíveis neste procedimento não forem flexíveis o suficiente para atender aos seus requisitos, opções de configuração adicionais podem ser aplicadas usando os `audit-destinations` endpoints, que estão na seção 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 servidor de auditoria e syslog, selecione **Configurar servidor syslog externo**. Ou, se tiver configurado anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

   O assistente Configurar servidor syslog externo é exibido.

2. Para a etapa **Enter syslog info** 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.

   Recomenda-se a utilização de **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 a grade e o servidor syslog externo. Para obter mais informações, "Gerenciar certificados de segurança"consulte .

   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 Protocolo de Registro de Eventos confiável (RELP) estende a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. O uso do RELP pode ajudar a evitar a perda de informações de auditoria se o servidor syslog externo tiver que reiniciar.

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

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

7. Selecione **continuar**.

Gerenciar o conteúdo do syslog

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

Passos

1. Para a etapa **Manage syslog Content** do assistente, selecione cada tipo de informação de auditoria que deseja enviar para o 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 entrar ou um usuário faz login como root

- * Enviar logs de aplicativos*: Envia arquivos de log úteis para solução de problemas, incluindo:
  - `bycast-err.log`
  - `bycast.log`
  - `jaeger.log`
  - `nms.log` (Somente nós de administração)
  - `prometheus.log`
  - `raft.log`
  - `hagroups.log`

Para obter informações sobre os logs do software StorageGRID, "Registos do software StorageGRID"consulte .

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

   Definir os valores de gravidade e facilidade pode ajudá-lo a agregar os logs de maneiras personalizáveis para facilitar a análise.

   a. Para **severidade**, selecione **passagem** ou selecione um valor de gravidade entre 0 e 7.

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

Gravidade	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de gravidade que 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 severidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA dá um valor de "info", enquanto parar intencionalmente o serviço SSM ou RSM dá um valor de "notice".
0	Emergência: O sistema não pode ser utilizado
1	Alerta: A 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	Debug: Mensagens no nível de depuração

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

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

Instalação	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de instalação que quando foi registrada localmente no nó: • Para logs de auditoria, a instalação enviada para o servidor syslog externo é "local7". • Para eventos de segurança, os valores das instalações são gerados pela distribuição linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação: ◦ `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
0	kern (mensagens do kernel)
1	utilizador (mensagens no nível do utilizador)
2	e-mail
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)

Instalação	Descrição
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias de rede)
8	UUCP
9	cron (daemon de relógio)
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (auditoria de log)
14	alerta de registo (alerta de registo)
15	relógio (daemon de 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 da grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudá-lo a validar toda a 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 grade e que a mensagem foi processada conforme esperado.

Passos

1. Se você não quiser enviar mensagens de teste porque você 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 **Skip and finish**.

   Um banner verde indica que a configuração foi salva.

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

   Os resultados do teste aparecem continuamente na página até que você pare o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuam 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.

   "Solucionar problemas de um servidor syslog externo"Consulte para ajudá-lo a resolver quaisquer erros.

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

   Se você estiver usando UDP, verifique toda a sua infraestrutura de coleção de logs. O protocolo UDP não permite uma deteção de erros tão rigorosa como os outros protocolos.

6. Selecione **Parar e terminar**.

   Você será devolvido à página **servidor de auditoria e syslog**. Um banner verde indica que a configuração do servidor syslog foi salva.

   As informações de auditoria do StorageGRID não são enviadas para o 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 "Registos do software StorageGRID" são enviados.

O StorageGRID usa o padrão de destinos de auditoria de nó local e armazena as informações de auditoria no `/var/local/log/localaudit.log`.

Ao usar `/var/local/log/localaudit.log`o , as entradas de log de auditoria do Gerenciador de Grade e do Gerenciador de locatário podem ser enviadas para um nó de armazenamento. Você pode encontrar 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 estão disponíveis se tiver configurado um servidor syslog externo.

Passos

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

Somente nós locais e **servidor syslog externo** normalmente fornecem melhor desempenho.

Opção	Descrição
Somente nós locais (padrão)	As mensagens de auditoria, os logs de eventos de segurança e os logs de aplicativos não são enviados para os 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 no `/var/local/log/localaudit.log`. **Nota**: 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 para o log é de 21 arquivos. Quando a versão 22nd 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 de aplicativos são armazenados nos nós que as 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` arquivo está normalmente vazio ou ausente. Ele 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 só é ativada depois de ter configurado 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 para o 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 só é ativada depois de ter configurado um servidor syslog externo.

2. Selecione **Guardar**.

   É apresentada uma mensagem de aviso.

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

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

   Os novos registos são enviados para os destinos selecionados. Os registos existentes permanecem na sua localização atual.

Utilize a monitorização SNMP

Usar monitoramento SNMP: Visão geral

Se você quiser monitorar o StorageGRID usando o Protocolo de Gerenciamento de rede simples (SNMP), configure o agente SNMP incluído no StorageGRID.

- "Configure o agente SNMP"
- "Atualize o agente SNMP"

Recursos

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB do StorageGRID contém definições de tabela e notificação para alertas e alarmes. 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.

Veja "Acesse arquivos MIB" se você deseja baixar os arquivos MIB em seus nós de grade.

Inicialmente, o SNMP está desativado 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

Traps são notificações enviadas pelo agente SNMP que não requerem confirmação pelo sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu dentro do StorageGRID, como um alerta sendo acionado.

Traps são suportados em todas as três versões do SNMP.

Informa

Os informes são semelhantes aos traps, mas requerem reconhecimento pelo sistema de gestão. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenvia a informação até que uma confirmação seja recebida ou o valor máximo de tentativa tenha sido atingido.

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de intercetação 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, tem de "configure um silêncio"o alertar. As notificações de alerta são enviadas pelo "Nó Admin. Remetente preferido".

  Cada alerta é mapeado para um dos três tipos de armadilha com base no nível de gravidade do alerta: ActiveMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem acionar esses traps, consulte "Referência de alertas".

- Alguns "alarmes (sistema legado)" são acionados em níveis de gravidade especificados ou superiores.

  As notificações SNMP não são enviadas para cada alarme ou para cada gravidade do alarme.

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas (OBTER e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de carateres da comunidade	Cadeia de carateres da comunidade	Utilizador do modelo de segurança baseado no utilizador (USM)
Notificações (ARMADILHA e INFORMAÇÃO)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Utilizador 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 suporta o modo de suporte de transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é AES.

Configure 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

O agente SNMP do StorageGRID suporta SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, apenas é suportada a autenticação modelo de segurança do utilizador (USM).

Todos os nós na grade usam a mesma configuração SNMP.

Especifique a configuração básica

Como primeira etapa, habilite o agente StorageGRID SMNP e forneça informações básicas.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   A página do agente SNMP é exibida.

2. Para ativar o agente SNMP em todos os nós de grade, marque a caixa de seleção **Enable SNMP** (Ativar SNMP*).
3. Introduza as seguintes informações na secção Configuração básica.

Campo	Descrição
Contacto do sistema	Opcional. O Contato principal do sistema StorageGRID, que é retornado em mensagens SNMP como sysContact. Normalmente, o contacto do sistema é um endereço de correio eletrónico. Esse valor se aplica a todos os nós no sistema StorageGRID. **O contacto do sistema** pode ter um máximo de 255 carateres.

Campo	Descrição
Localização do sistema	Opcional. A localização do sistema StorageGRID, que é retornado em mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde o sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. Esse valor se aplica a todos os nós no sistema StorageGRID. **A localização do sistema** pode ter no máximo 255 carateres.
Ativar notificações de agente SNMP	• Se selecionado, o agente SNMP do StorageGRID envia trap e informa notificações. • Se não estiver selecionado, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.
Ativar traps de autenticação	Se selecionado, o agente SNMP do StorageGRID envia traps de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Introduza cadeias de carateres da comunidade

Se você usar SNMPv1 ou SNMPv2c, complete a seção cadeias de Comunidade.

Quando o sistema de gerenciamento consulta o MIB do StorageGRID, ele envia uma string de comunidade. Se a cadeia de carateres 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**, opcionalmente, insira uma cadeia de carateres comunitária para permitir acesso MIB somente leitura em endereços de agentes IPv4 e IPv6.

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

   Cada string de comunidade pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

2. Selecione **Adicionar outra string de comunidade** para adicionar strings adicionais.

   Até cinco cordas são permitidas.

Crie destinos de armadilha

Use a guia Trap Destinations (destinos de intercetação) na seção Other configurations (outras configurações) para definir um ou mais destinos para o StorageGRID trap (trap de intercetação) ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

Passos

1. Para o campo **Default trap Community** (comunidade de trap padrão), insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de trap SNMPv1 ou SNMPv2.

   Conforme necessário, você pode fornecer uma string de comunidade ("personalizada") diferente quando você define um destino de armadilha específico.

   A comunidade de trap padrão pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

2. Para adicionar um destino de armadilha, selecione **criar**.
3. Selecione a versão SNMP que será utilizada 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 armadilha para SNMPv1.
Host	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 padrão de intercetação SNMP, a menos que você precise usar TCP.
Cadeia de carateres da comunidade	Use a comunidade de trap padrão, se uma foi especificada, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço 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.
Host	Um endereço IPv4 ou IPv6 ou 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 padrão de intercetação SNMP, a menos que você precise usar TCP.
Cadeia de carateres da comunidade	Use a comunidade de trap padrão, se uma foi especificada, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço 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.
Host	Um endereço IPv4 ou IPv6 ou 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 padrão de intercetação SNMP, a menos que você precise usar TCP.
Utilizador USM	O utilizador USM que será utilizado para autenticação. • Se selecionou **Trap**, apenas são apresentados utilizadores USM sem IDs de motor autoritativas. • Se selecionou **inform**, apenas são apresentados utilizadores USM com IDs de motor autoritativas. • Se não forem apresentados utilizadores: i. Crie e salve o destino da armadilha. ii. Vá para Crie utilizadores USM e crie o usuário. iii. Regresse ao separador Trap Destinations (destinos da armadilha), selecione o destino guardado na tabela e selecione **Edit** (Editar). iv. Selecione o utilizador.

5. Selecione **criar**.

   O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agente

Opcionalmente, use a guia endereços de agentes na seção outras configurações para especificar um ou mais "endereços de escuta". Estes 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. Introduza as seguintes informações.

Campo	Descrição
Protocolo da Internet	Se esse endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se esse endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Qual rede StorageGRID o agente ouvirá. • Redes Grid, Admin e Client: O agente SNMP escutará consultas em todas as três redes. • Rede de rede • Rede de administração • Rede de clientes **Nota**: 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 que o agente SNMP deve ouvir. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Nota**: 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.

Crie utilizadores USM

Se estiver a utilizar o SNMPv3, utilize o separador utilizadores USM na secção outras configurações para definir os utilizadores USM que estão autorizados a consultar o MIB ou a receber traps e informações.

SNMPv3 *inform* destinos devem ter usuários com IDs de motor. SNMPv3 *trap* destino não pode ter usuários com IDs de motor.

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

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Nome de utilizador	Um nome exclusivo para este utilizador USM. Os nomes de usuário podem ter um máximo de 32 carateres e não podem conter carateres de espaço em branco. O nome de usuário não pode ser alterado depois que o usuário é criado.
Acesso MIB somente leitura	Se selecionado, este utilizador deverá ter acesso apenas de leitura à MIB.
ID do motor autoritário	Se este utilizador for utilizado num destino de informação, o ID de mecanismo autorizado para este utilizador. Insira 10 a 64 carateres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para utilizadores USM que serão selecionados em destinos de armadilha para informação. Este valor não é permitido para utilizadores USM que serão selecionados em destinos de armadilha para armadilhas. **Nota**: Este campo não é mostrado se você selecionou **Acesso MIB somente leitura** porque os usuários USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o utilizador USM: • **AuthPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe, um protocolo de privacidade e uma palavra-passe. • **AuthNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Palavra-passe	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Mostrado apenas se você selecionou **authPriv** e sempre definido como AES, que é o único protocolo de privacidade suportado.
Palavra-passe	Mostrado apenas se você selecionou **authPriv**. A senha que este usuário usará para privacidade.

3. Selecione **criar**.

   O utilizador USM é criado e adicionado à tabela.

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

A nova configuração do agente SNMP fica ativa.

Atualize o agente SNMP

Você pode desativar notificações SNMP, atualizar strings da comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de intercetação.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Consulte "Configure 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 as alterações feitas em cada guia.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   A página do agente SNMP é exibida.

2. Para desativar o agente SNMP em todos os nós de grade, desmarque a caixa de seleção **Ativar 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 **localização do sistema**.
   b. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar notificações de agente SNMP** para controlar se o agente StorageGRID SNMP envia trap e informa notificações.

      Quando esta caixa de verificação 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 traps de autenticação** para controlar se o agente SNMP do StorageGRID envia traps 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 cadeias de Comunidade.
5. Para atualizar destinos de intercetação, selecione a guia destinos de intercetação na seção outras configurações.

   Utilize este separador para definir um ou mais destinos para o StorageGRID trap ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

   Para obter detalhes sobre o que introduzir, "Criar destinos de armadilha"consulte .

   - Opcionalmente, atualize ou remova a comunidade de trap padrão.

     Se você remover a comunidade de trap padrão, primeiro deve garantir que todos os destinos de trap

existentes usem uma cadeia de carateres 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 guia para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

   Para obter detalhes sobre o que introduzir, "Criar endereços de agente"consulte .

   - Para adicionar um endereço de agente, selecione **criar**.
   - Para editar um endereço de 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 os utilizadores USM, selecione o separador utilizadores USM na secção outras configurações.

   Utilize este separador para definir os utilizadores USM que estão autorizados a consultar a MIB ou a receber traps e informações.

   Para obter detalhes sobre o que introduzir, "Crie utilizadores USM"consulte .

   - Para adicionar um utilizador USM, selecione **criar**.
   - Para editar um utilizador USM, selecione o botão de opção e selecione **Edit**.

     O nome de utilizador de um utilizador USM existente não pode ser alterado. Se você precisar alterar um nome de usuário, você deve remover o usuário e criar um novo.

     > Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, você deverá editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

   - Para remover um utilizador USM, selecione o botão de opção e selecione **Remover**.

     > Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deve editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando tiver atualizado a configuração do agente SNMP, selecione **Save**.

Acesse arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e

serviços gerenciados para os nós em sua grade. Você pode acessar arquivos MIB que definem os objetos e notificações do StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Consulte "Utilize a monitorização SNMP" para obter mais informações sobre ficheiros SNMP e MIB.

Acesse arquivos MIB

Siga estes passos para aceder aos ficheiros MIB.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
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 em série e.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com 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 StorageGRID do arquivo MIB:

   a. Obtenha o OID da raiz do MIB do StorageGRID:

   ```
   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` comando tem muitas opções que são 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	Código Objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID.

Objetos MIB

Nome do objeto	Código Objeto (OID)	Descrição
ActiveAlertCount		O número de alertas ativos na activeAlertTable.
ActiveAlertTable		Uma tabela de alertas ativos no StorageGRID.
ActiveAlertId		O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
ActiveAlertName		O nome do alerta.
ActiveAlertInstance		O nome da entidade que gerou o alerta, normalmente o nome do nó.
ActiveAlertSeverity		A gravidade do alerta.
ActiveAlertStartTime		A data e a hora em que o alerta foi acionado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo de notificação	Código Objeto (OID)	Descrição
ActiveMinorAlert		Um alerta com gravidade menor
ActiveMajorAlert		Um alerta com grande gravidade
ActiveCriticalAlert		Um alerta com gravidade crítica

Colete dados adicionais do StorageGRID

Use gráficos e gráficos

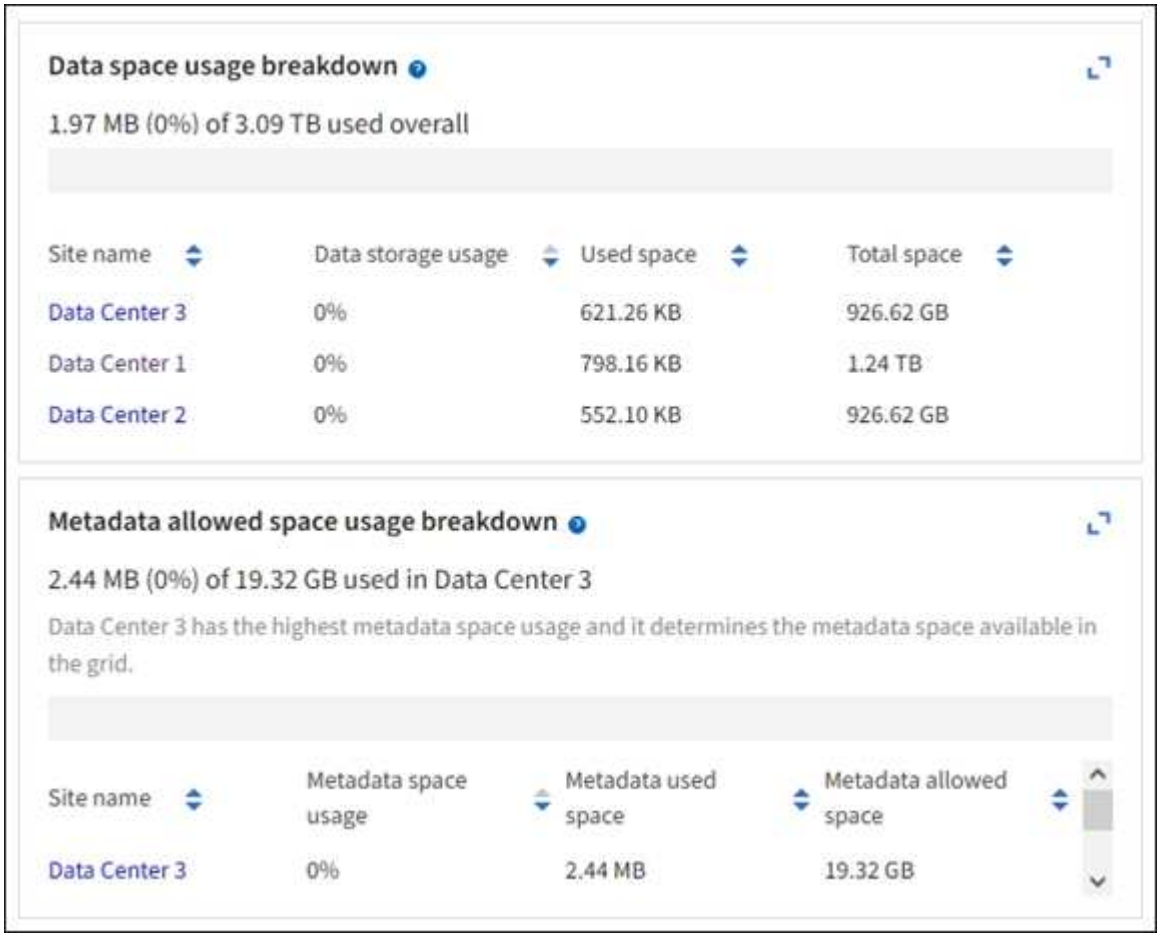
Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas.

O Gerenciador de Grade é atualizado com cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

Tipos de gráficos

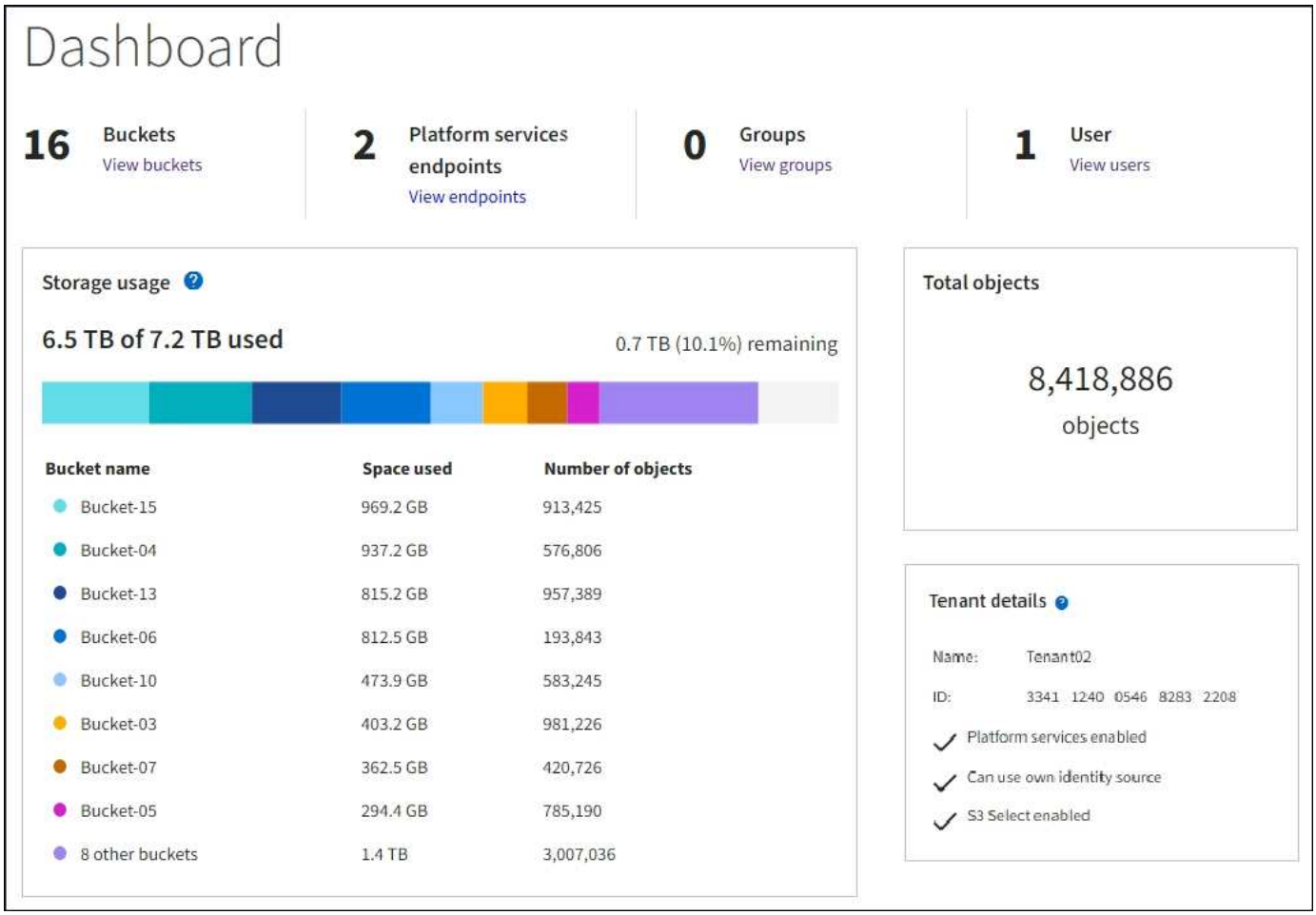
Gráficos e gráficos resumem os valores de métricas e atributos específicos do StorageGRID.

O painel do Gerenciador de Grade inclui cartões que resumem o armazenamento disponível para a grade e cada local.



O painel uso do armazenamento no painel do Gerenciador do locatário exibe o seguinte:

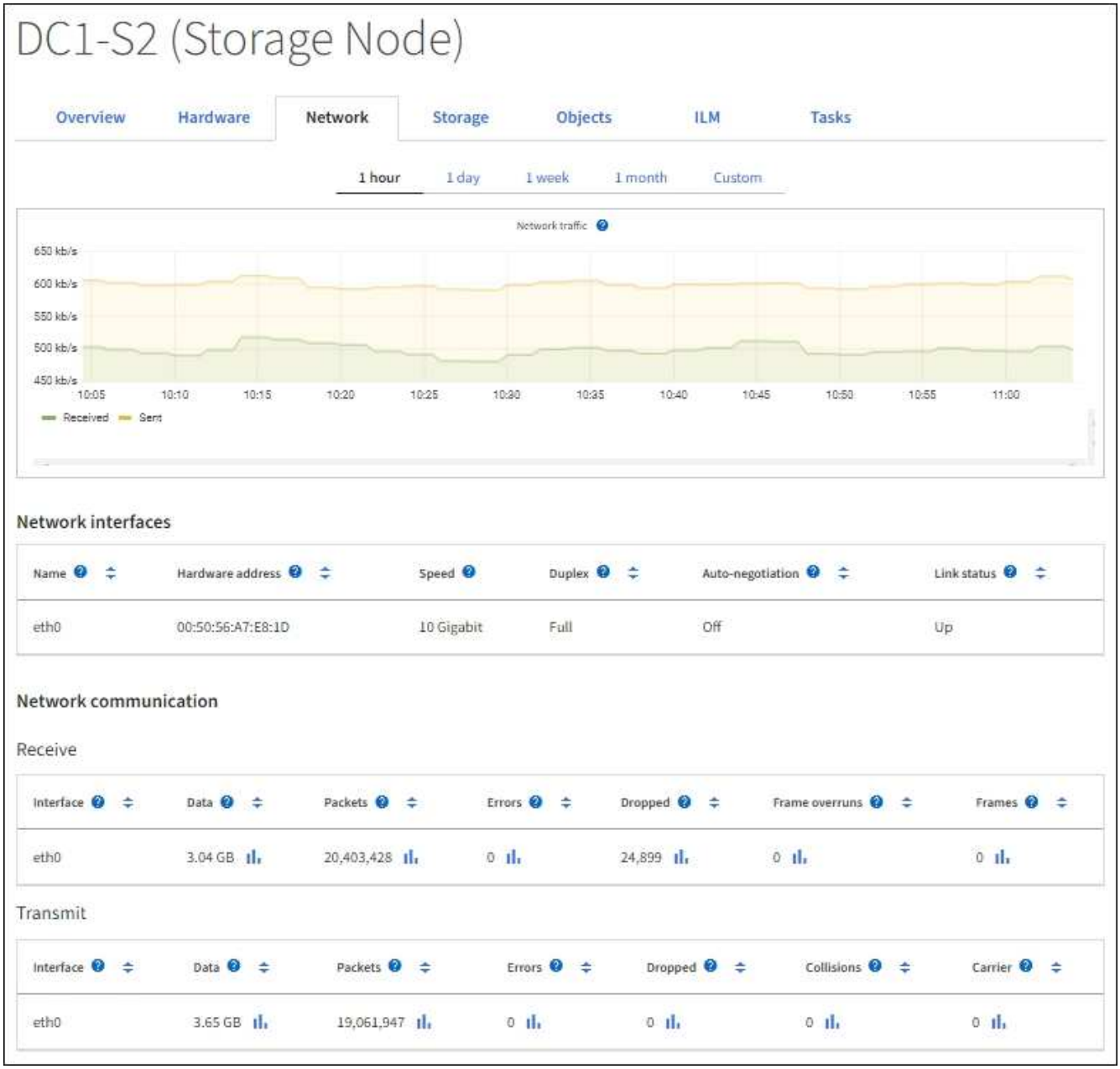
- Uma lista dos maiores baldes (S3) ou contentores (Swift) para o inquilino
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores
- A quantidade total de espaço utilizado e, se for definida uma quota, a quantidade e a percentagem de espaço restante



Além disso, gráficos que mostram como as métricas e atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topology**.

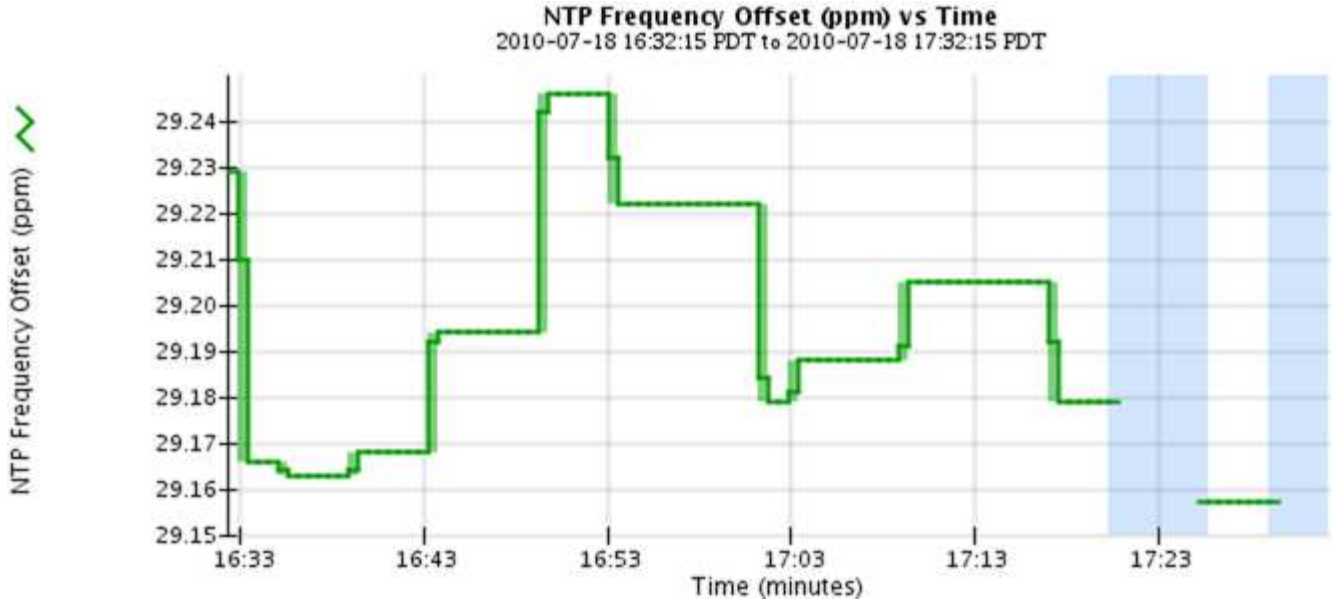
Existem quatro tipos de gráficos:

- **Gráficos Grafana**: Mostrados na página de nós, gráficos Grafana são usados para plotar os valores das métricas Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **rede** para um nó de armazenamento inclui um gráfico Grafana para tráfego de rede.

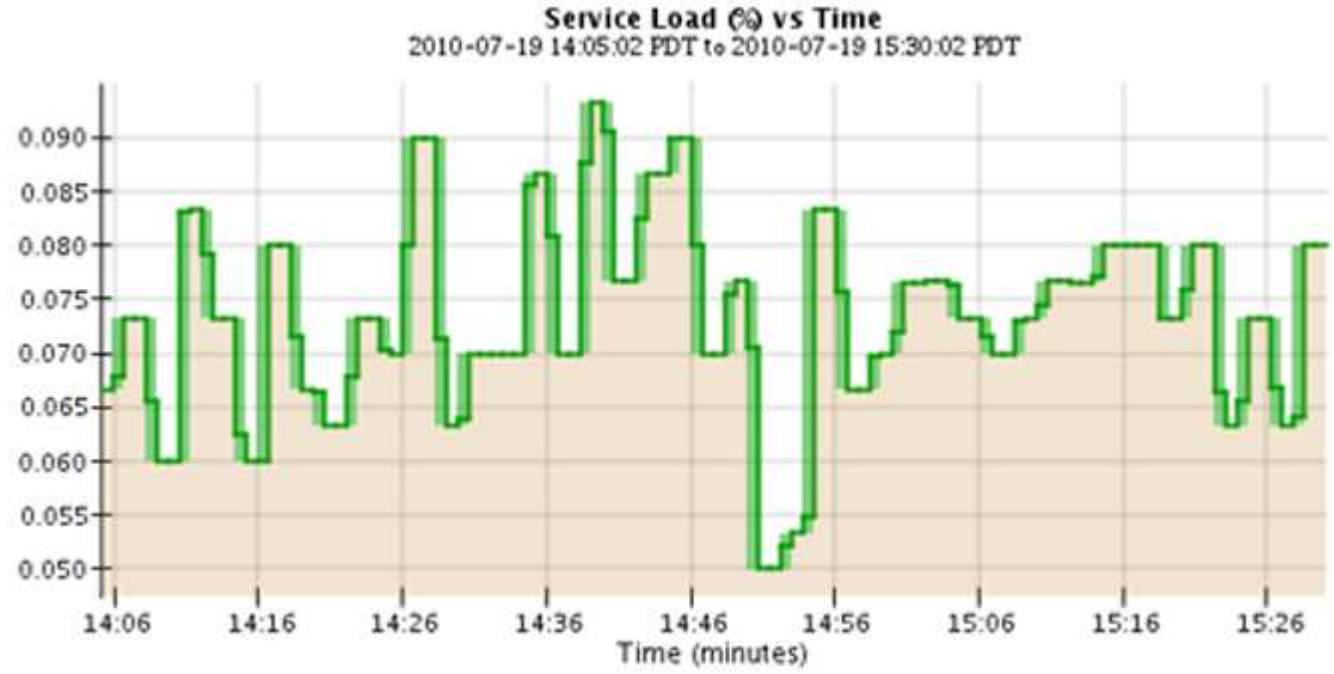


Gráficos Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPPORT** > **Tools** > **Metrics**.

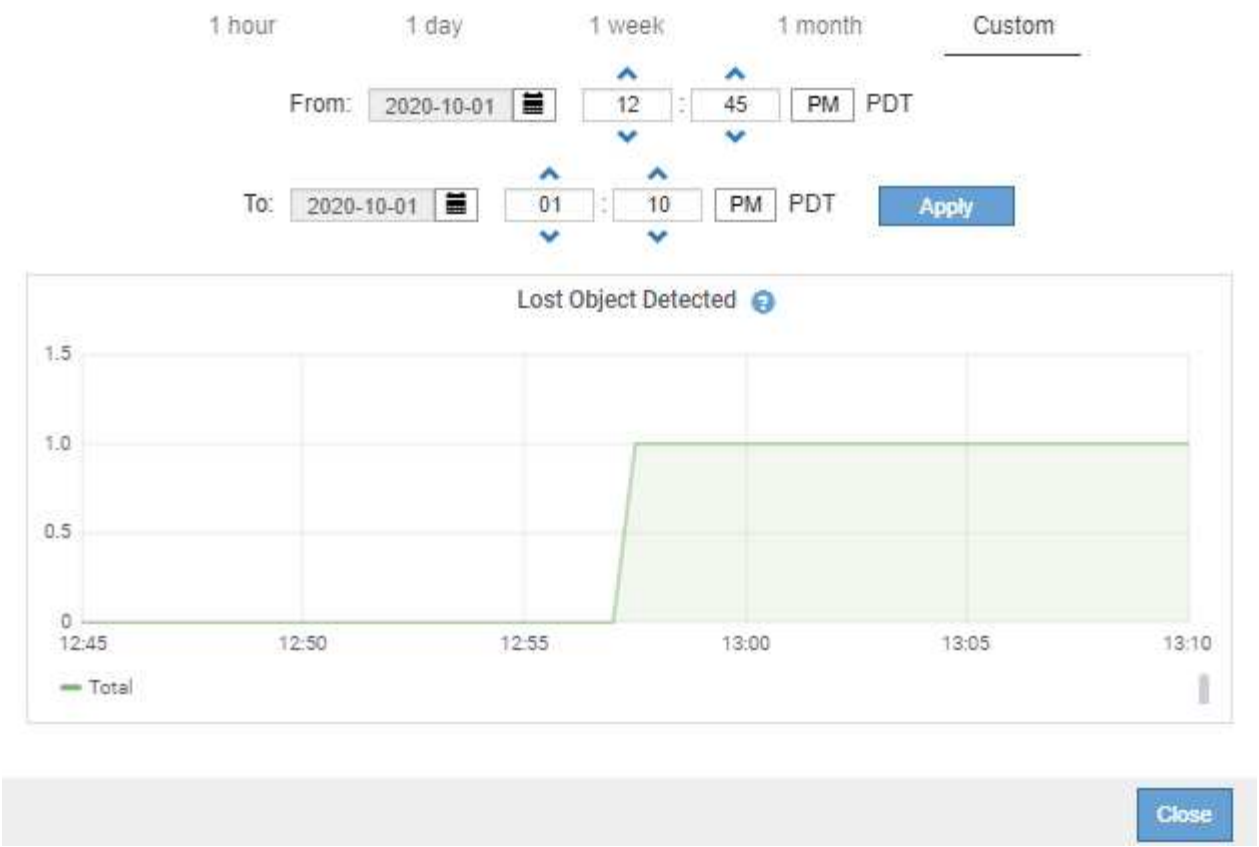
- **Gráficos de linha**: Disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topoly** (selecione o ícone do gráfico após um valor de dados), os gráficos de linha são usados para plotar os valores dos atributos StorageGRID que têm um valor unitário (como deslocamento de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



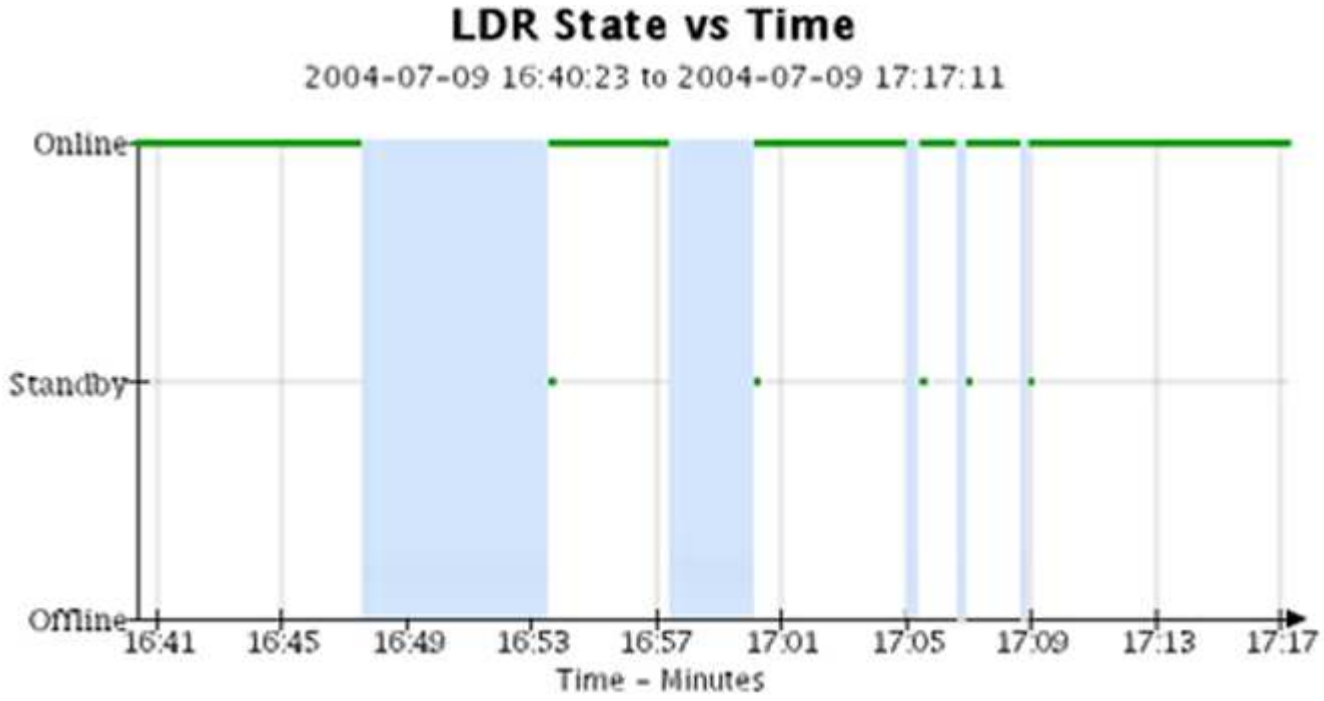
- **Gráficos de área**: Disponíveis na página de nós e na página **SUPPORT** > **Tools** > **Grid topology** (selecione o ícone do gráfico após um valor de dados), os gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. Os gráficos de área são semelhantes aos gráficos de linha, 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 denotados com um tipo diferente de ícone de gráfico e têm um formato diferente:



- **State graph**: Disponível na página **SUPPORT** > **Tools** > **Grid topoly** (selecione o ícone do gráfico após um valor de dados), os gráficos de estado são usados para plotar valores de atributo que representam estados distintos, como um estado de serviço que pode ser on-line, standby 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

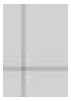
"Exibir a página nós"

"Veja a árvore de topologia de Grade"

"Analise as métricas de suporte"

Legenda da carta

As linhas e cores usadas para desenhar gráficos têm significado específico.

Exemplo	Significado
	Os valores de atributo relatados são plotados usando linhas verdes escuras.
	O sombreamento verde claro em torno de linhas verdes escuras indica que os valores reais nesse intervalo de tempo variam e foram "encadernados" para 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 castanho claro é usado para gráficos de área para indicar dados volumétricos.
	Áreas em branco (sem dados plotados) indicam que os valores do atributo 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 do 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 atributo naquele momento não eram conhecidos porque o serviço que relata os atributos estava administrativamente inativo.
	Uma mistura de sombreamento cinza e azul indica que alguns dos valores de atributo na época eram indeterminados (porque o serviço estava em um estado desconhecido), enquanto outros não eram conhecidos porque o serviço relatando os atributos estava administrativamente para baixo.

Apresentar gráficos e gráficos

A página nós contém os gráficos e gráficos que você deve acessar regularmente para monitorar atributos como capacidade de storage e taxa de transferência. Em alguns casos, especialmente ao trabalhar com suporte técnico, você pode usar a página **SUPPORT** > **Tools** > **Grid topology** para acessar gráficos adicionais.

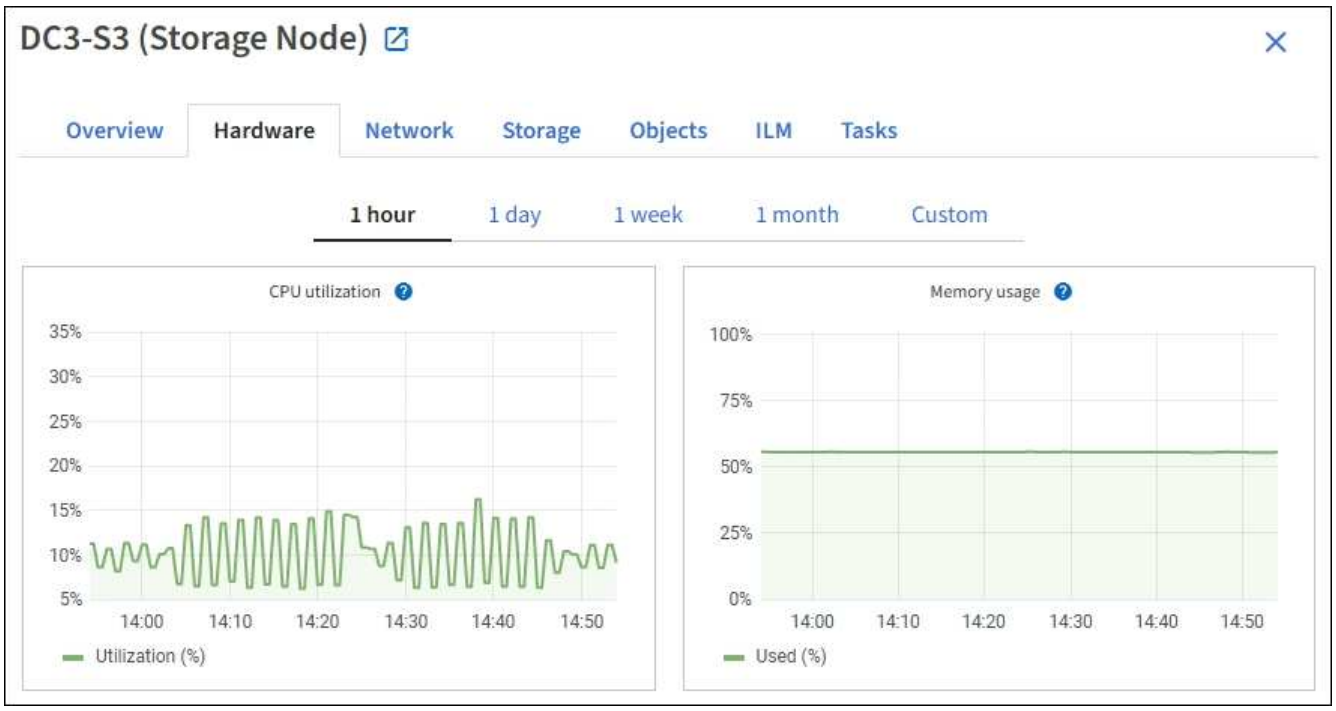
Antes de começar

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

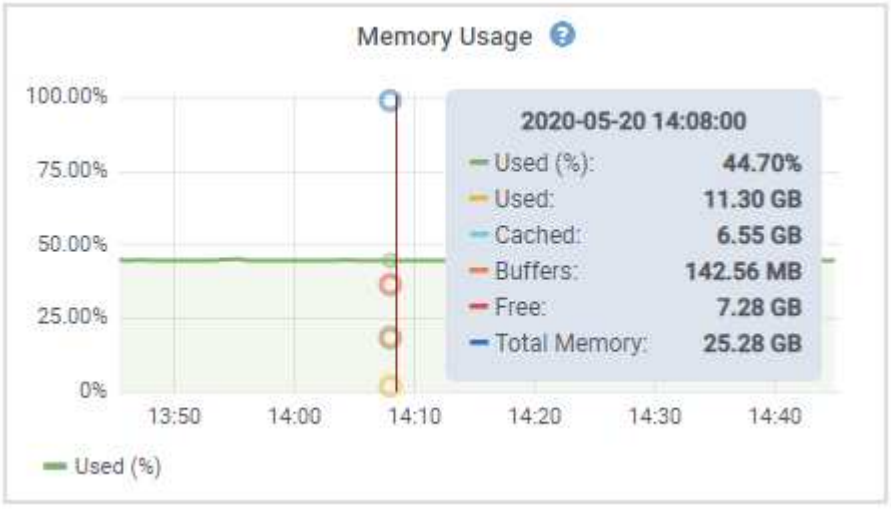
Passos

1. Selecione **NODES**. Em seguida, selecione um nó, um site ou toda a grade.
2. Selecione o separador para o qual pretende ver as informações.

Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas de Prometheus ao longo do tempo. Por exemplo, a guia **NÓS** > **hardware** de um nó inclui dois gráficos Grafana.



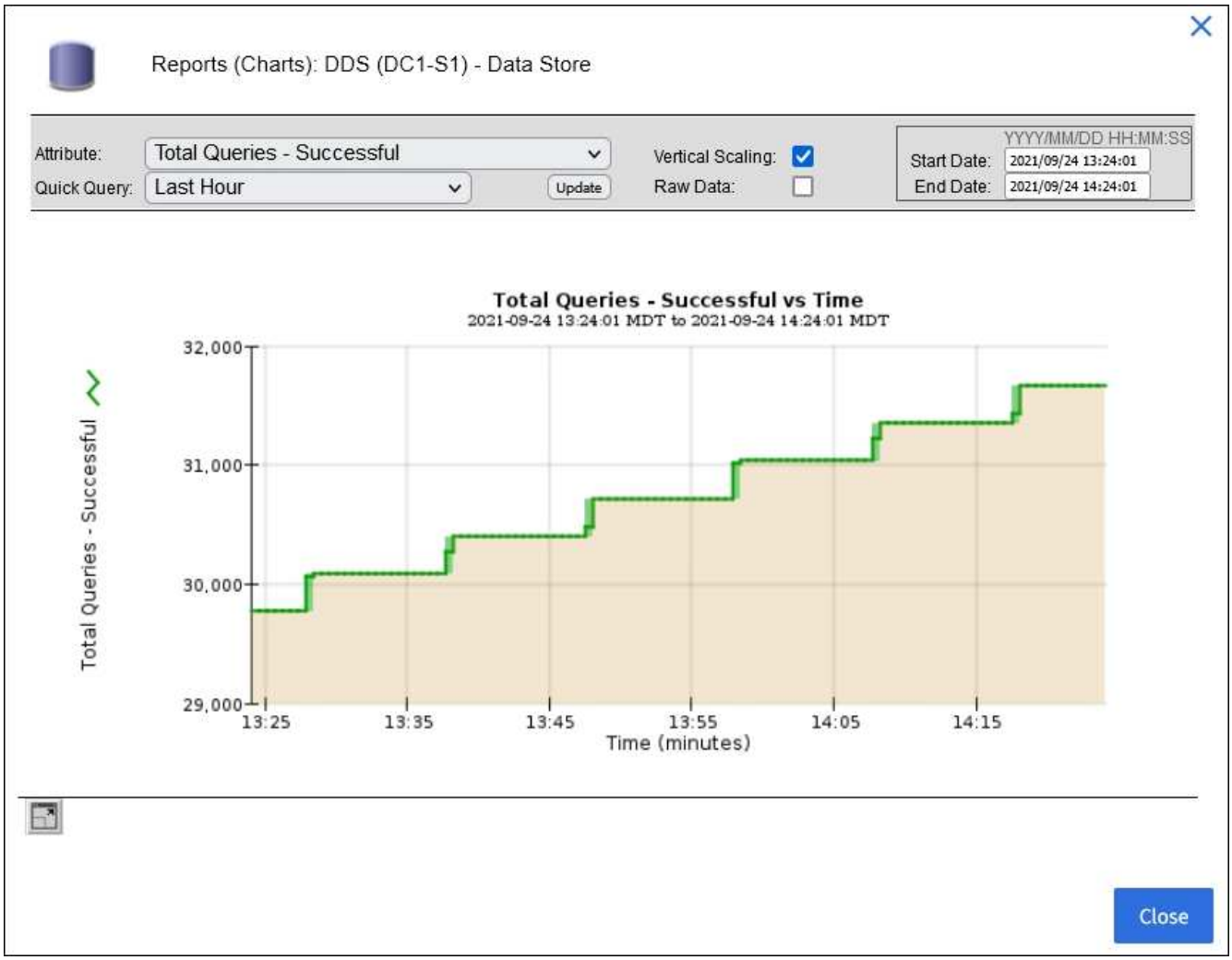
3. Opcionalmente, posicione o cursor sobre o gráfico para ver valores mais detalhados para um determinado ponto no tempo.

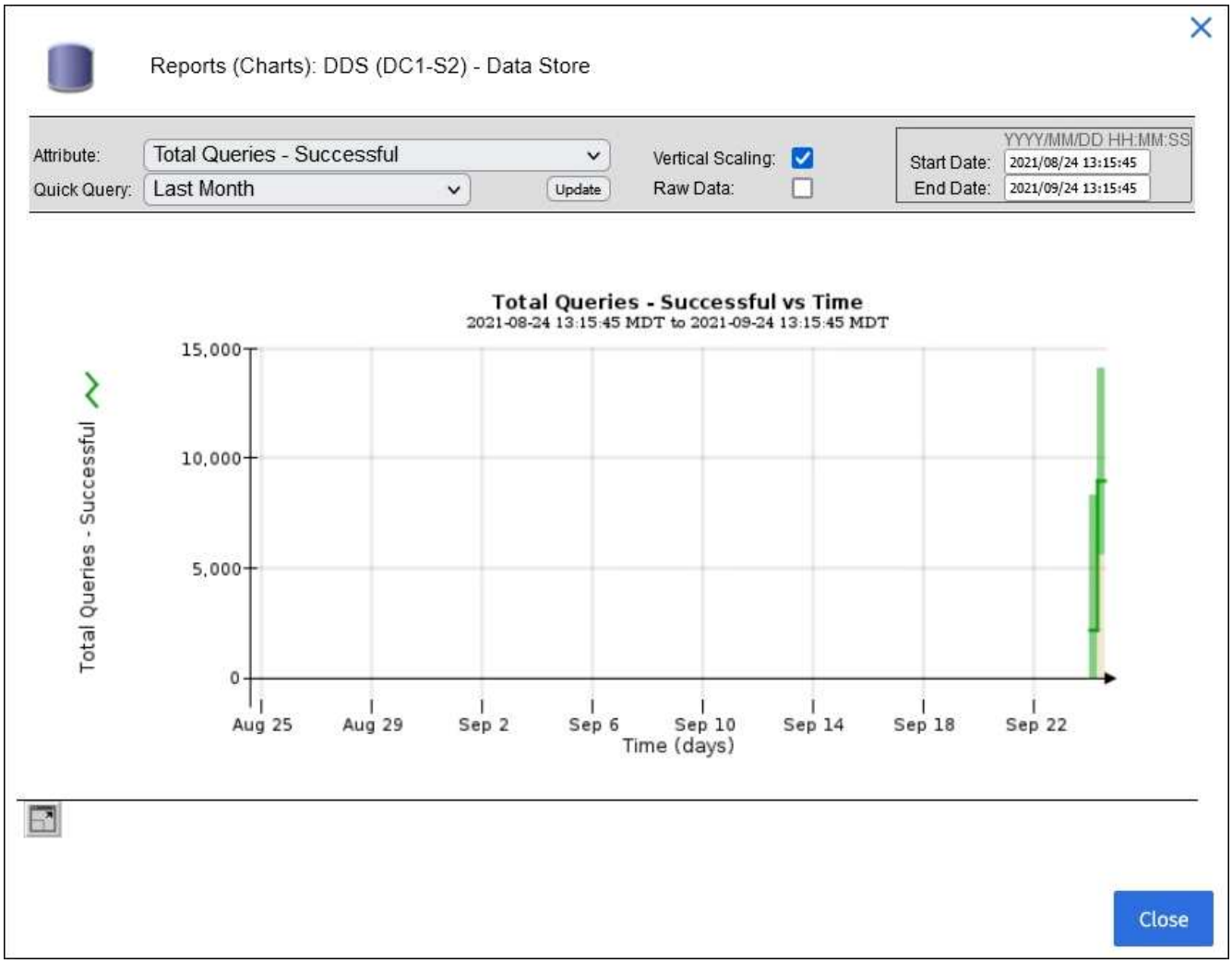


4. Conforme necessário, muitas vezes é possível exibir um gráfico para um atributo ou métrica específico. Na tabela na página nós, selecione o ícone do gráfico à direita do nome do atributo.

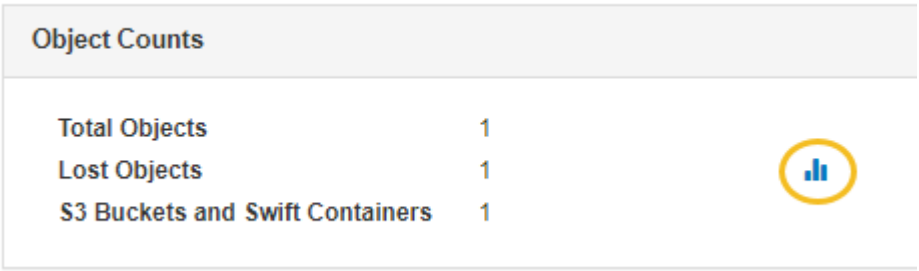
> Os gráficos não estão disponíveis para todas as métricas e atributos.

Exemplo 1: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o número total de consultas de armazenamento de metadados bem-sucedidas para o nó de armazenamento.

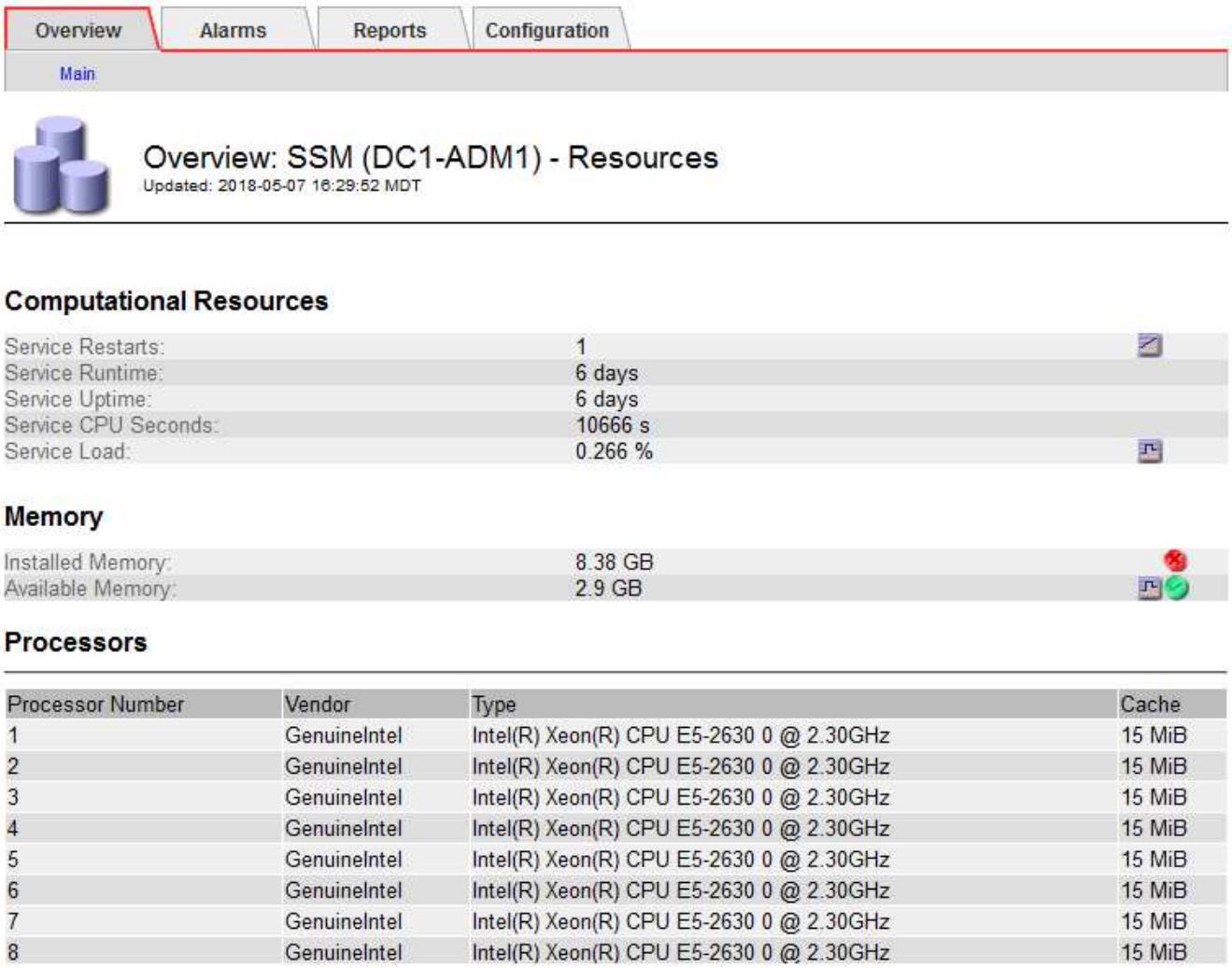

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 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 detetados ao longo do tempo.



5. Para exibir gráficos para atributos que não são exibidos na página nó, selecione **support** > **Tools** > **Grid topoly**.
6. Selecione ***grid node*** > ***component ou Service*** > **Overview** > **Main**.



7. Selecione o ícone do gráfico ao lado do atributo.

   O visor 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 em um local de data center, nó de grade, componente ou serviço.

Antes de começar

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

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > ***component ou Service*** > **Reports** > **Charts**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Para forçar o eixo Y a iniciar em zero, desmarque a caixa de seleção **vertical Scaling**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **dados brutos** ou arredondar valores

para um máximo de três casas decimais (por exemplo, para atributos reportados 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 após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, personalize o período de tempo para o gráfico inserindo **Data de início** e **Data de término**.

   Utilize o formato *YYYY/MM/DDHH:MM:SS* na hora 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. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.

Use relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Existem 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 agregados para períodos de tempo superiores a uma semana.

Relatórios de texto bruto

Um relatório de texto bruto exibe detalhes sobre o atributo selecionado:

- Hora recebida: Data e hora local 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 tempo 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 %

Agregar relatórios de texto

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 de resumir vários valores de atributo (um agregado de valores de atributo) pelo serviço NMS ao longo do tempo em uma única entrada com valores médios, máximos e mínimos que são derivados da agregação.

Cada entrada exibe as seguintes informações:

- Hora agregada: Data e hora locais da última vez que o serviço NMS agregou (coletou) um conjunto de valores de atributo alterados.
- Valor médio: A média do valor do atributo durante o período de tempo agregado.
- Valor mínimo: O valor mínimo durante o 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 em um local de data center, nó de grade, componente ou serviço.

Antes de começar

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

Sobre esta tarefa

Para dados de atributos que se espera que estejam mudando continuamente, esses dados de atributo são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributos 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 apresentado depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos de tempo superiores a uma semana.

Texto cinza indica que o serviço foi desativado administrativamente durante o período de amostragem. Texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > ***component ou Service*** > **Reports** > **Text**.
3. Selecione o atributo para relatar 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 reportados 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 após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, você precisa personalizar o período de tempo para relatar inserindo **Data de início** e **Data de término**.

   Utilize o formato `YYYY/MM/DDHH:MM:SS` na hora 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 momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.

Exportar relatórios de texto

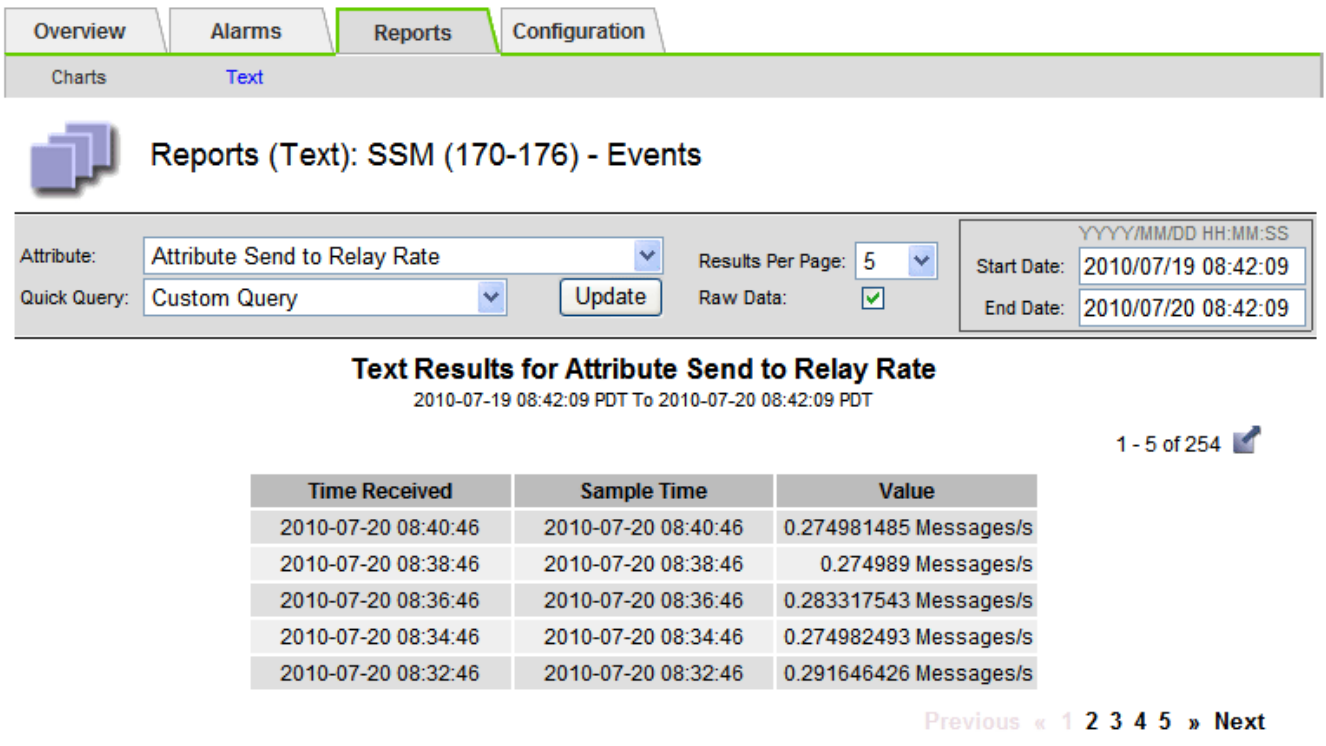
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

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 **SUPPORT** > **Tools** > **Grid topology**.
2. Crie um relatório de texto.
3. Clique em *Exportar*.



A janela Exportar relatório de texto abre-se 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 podem agora ser colados em um documento de terceiros, como uma Planilha.

Monitore O PUT e obtenha desempenho

Você pode monitorar o desempenho de certas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir mais investigação.

Sobre esta tarefa

Para monitorar O desempenho, você pode executar comandos S3 e Swift 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 and GET, use as seguintes diretrizes:

- Use tamanhos de objeto comparáveis aos objetos que você normalmente ingere em sua grade.
- Realize operações em locais locais e remotos.

As mensagens na "log de auditoria" indicam o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação GET S3, 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:

- **S3**: EXCLUIR, OBTER, CABEÇA, METADADOS ATUALIZADOS, POSTAR, COLOCAR
- **SWIFT**: EXCLUIR, OBTER, CABEÇA, COLOCAR

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o throughput geral que você pode alcançar. Repita os mesmos testes regularmente e registe os resultados, para

que possa identificar tendências que possam necessitar de investigação.

- Você pode "Baixe S3tester a partir de github".

Monitorar operações de verificação de objetos

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".

Sobre esta tarefa

Dois "processos de verificação" trabalham juntos para garantir a integridade dos dados:

- * A verificação em segundo plano* é executada automaticamente, verificando continuamente a correção dos dados do objeto.

  A verificação em segundo plano verifica automaticamente e continuamente todos os nós de storage para determinar se há cópias corrompidas de dados de objetos replicados e codificados por apagamento. Se forem encontrados problemas, o sistema StorageGRID tentará substituir automaticamente os dados de objetos corrompidos de cópias armazenadas em outro lugar do sistema. A verificação em segundo plano não é executada em nós de arquivamento ou em objetos em um pool de storage de nuvem.

  > ⓘ O alerta **Objeto corrompido não identificado detetado** é acionado se o sistema detetar 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 (embora não a correção) de dados de objetos.

  A verificação de existência de objeto verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados por apagamento existem em um nó de storage. A verificação de existência de objeto fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware poderia ter afetado a integridade dos dados.

Você deve rever os resultados de verificações de antecedentes e verificações de existência de objetos regularmente. Investigue quaisquer instâncias de dados de objetos corrompidos ou ausentes imediatamente para determinar a causa raiz.

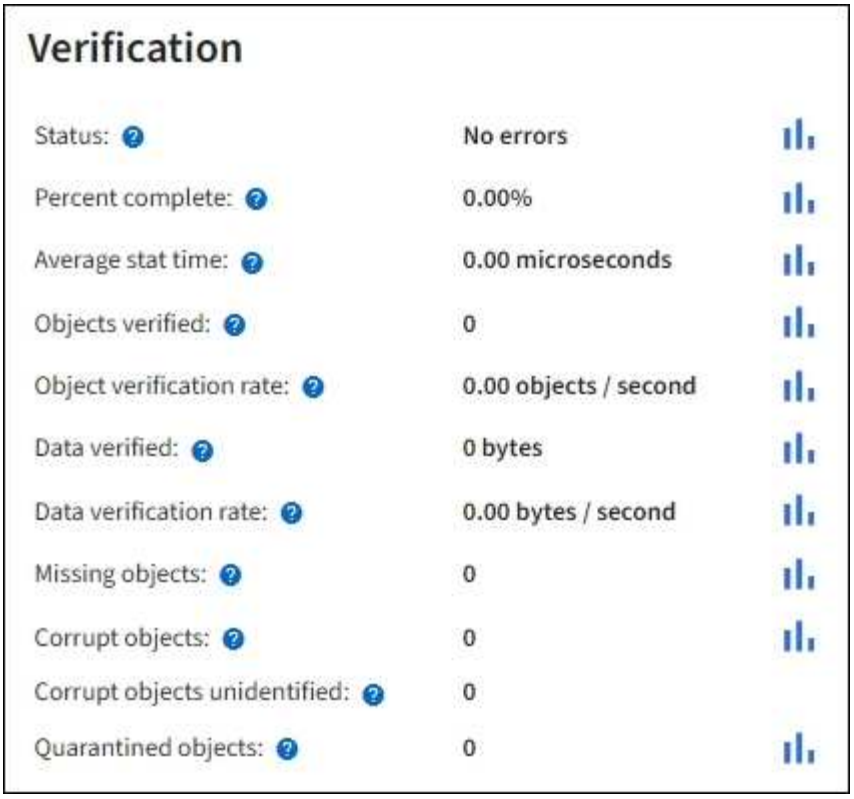
Passos

1. Reveja os resultados das verificações de antecedentes:

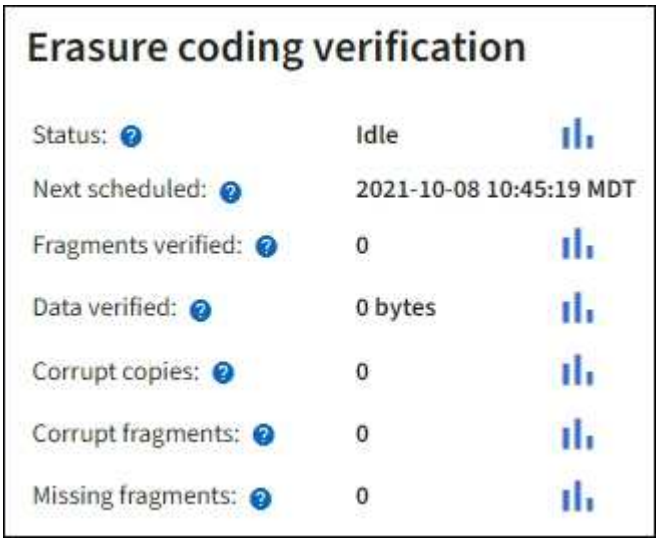
   a. Selecione **NODES** > ***Storage Node*** > **Objects**.

   b. Verifique os resultados da verificação:

      - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.

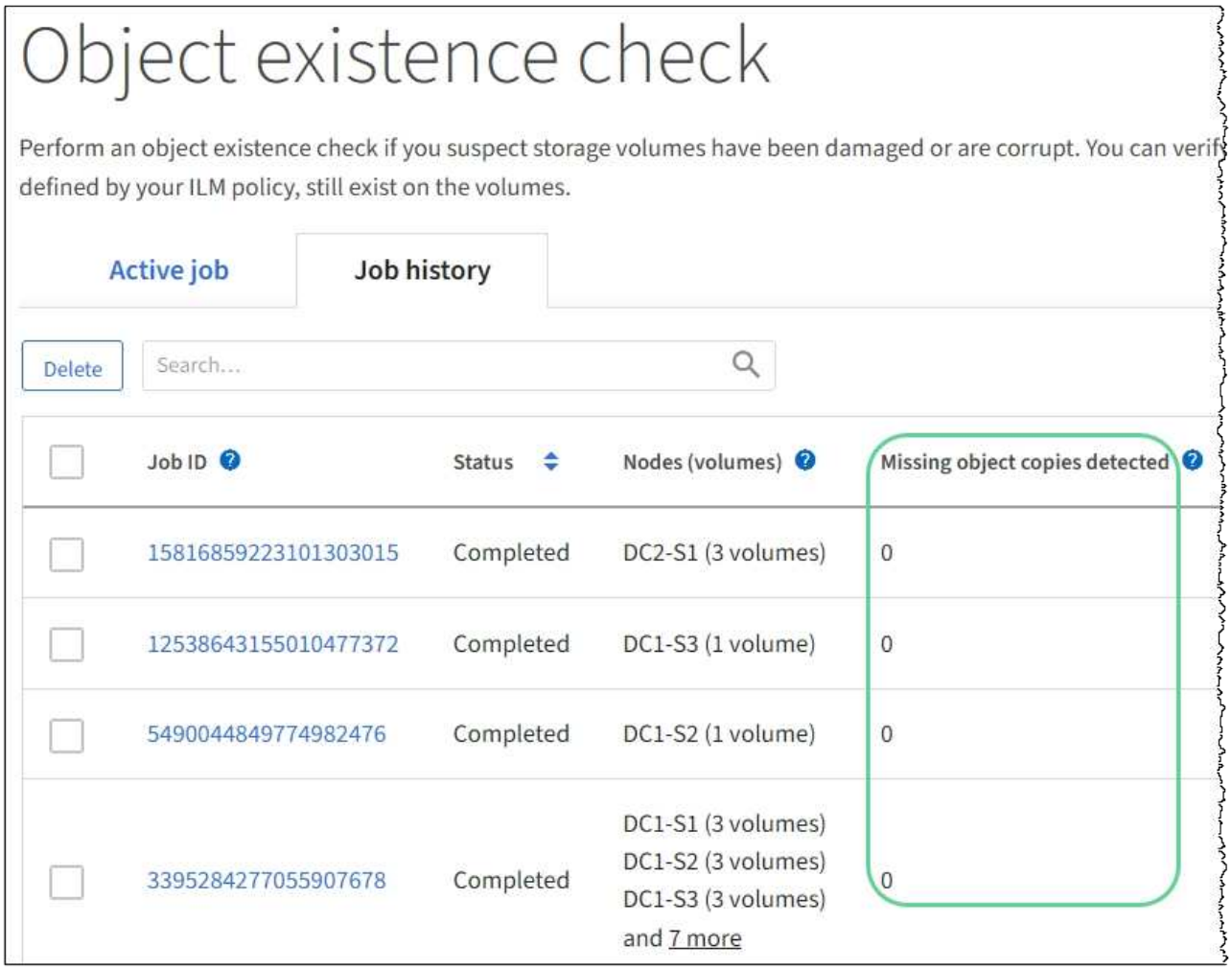


- Para verificar a verificação de fragmentos codificados por apagamento, selecione ***Storage Node*** > **ILM** e veja os atributos na seção de verificação de codificação de apagamento.



Selecione o ponto de interrogação ao lado do nome de um atributo para exibir o texto da ajuda.

2. Reveja os resultados dos trabalhos de verificação de existência de objeto:
   a. Selecione **MAINTENANCE** > **Object existence check** > **Job history**.
   b. Digitalizar a coluna cópias de objeto em falta detetadas. Se algum trabalho resultar em 100 ou mais cópias de objetos ausentes e o alerta **objetos perdidos** tiver sido acionado, entre em Contato com o suporte técnico.



Monitorar eventos

Você pode monitorar eventos que são detetados por um nó de grade, incluindo eventos personalizados que você criou para rastrear eventos registrados no servidor syslog. A mensagem último evento mostrada no Gerenciador de Grade fornece mais informações sobre o evento mais recente.

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

O alarme SMTT (Total de eventos) pode ser repetidamente acionado por problemas como problemas de rede, interrupções de energia ou atualizações. Esta seção tem informações sobre a investigação de 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 de grade:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   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 **SUPPORT** > **Tools** > **Grid topology**.

b. Selecione ***site*** > ***grid node*** > **SSM** > **Eventos** > **relatórios**.

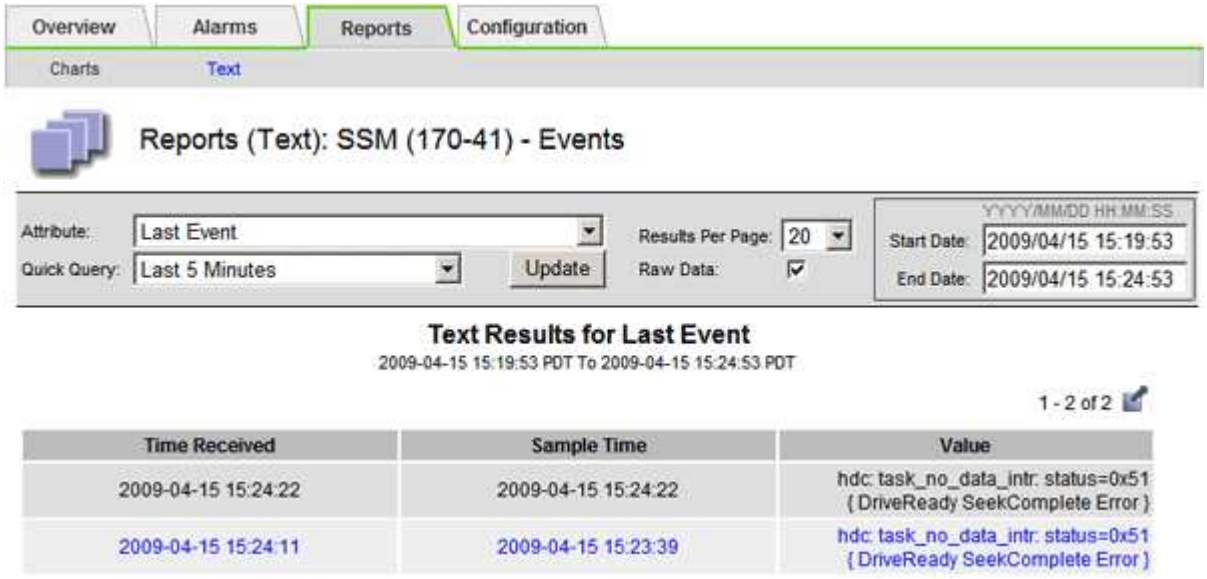
c. Selecione **texto**.

O atributo **último evento** não é mostrado no "vista de gráficos". Para visualizá-lo:

d. Altere **Atributo** para **último evento**.

e. Opcionalmente, selecione um período de tempo para **consulta rápida**.

f. Selecione **Atualizar**.



Crie eventos syslog personalizados

Eventos personalizados permitem que você acompanhe todos os eventos de usuário do kernel, daemon, erro e nível crítico 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.

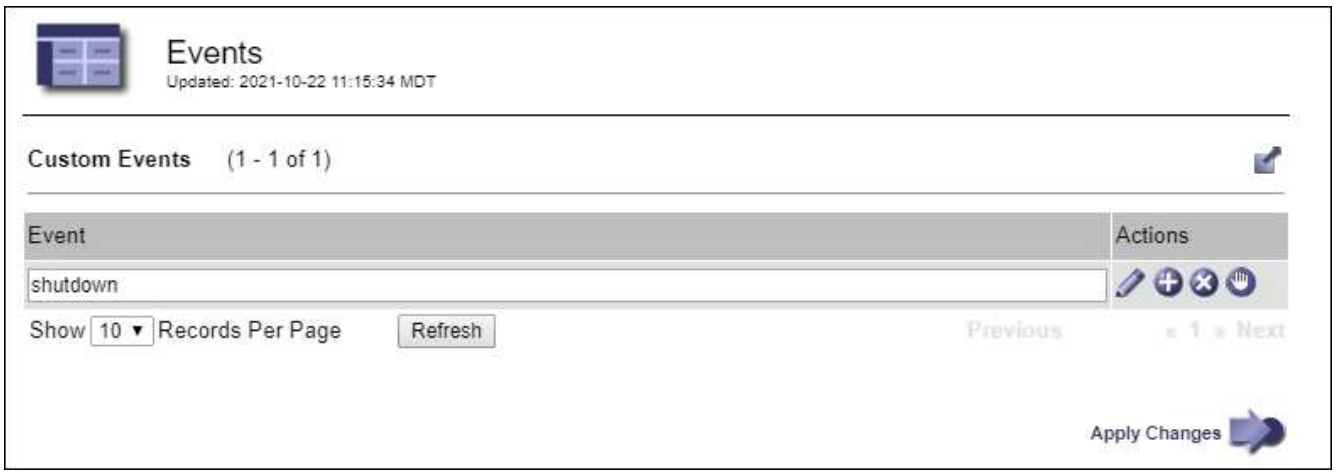
- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada.
- Para criar um evento personalizado com base em palavras-chave nos `/var/local/log/messages` arquivos, os logs nesses arquivos devem ser:
  - Gerado pelo kernel
  - Gerado pelo daemon ou programa do usuário no nível de erro ou crítico

Nota: nem todas as entradas nos `/var/local/log/messages` arquivos serão correspondidas a menos que satisfaçam os requisitos acima indicados.

Passos

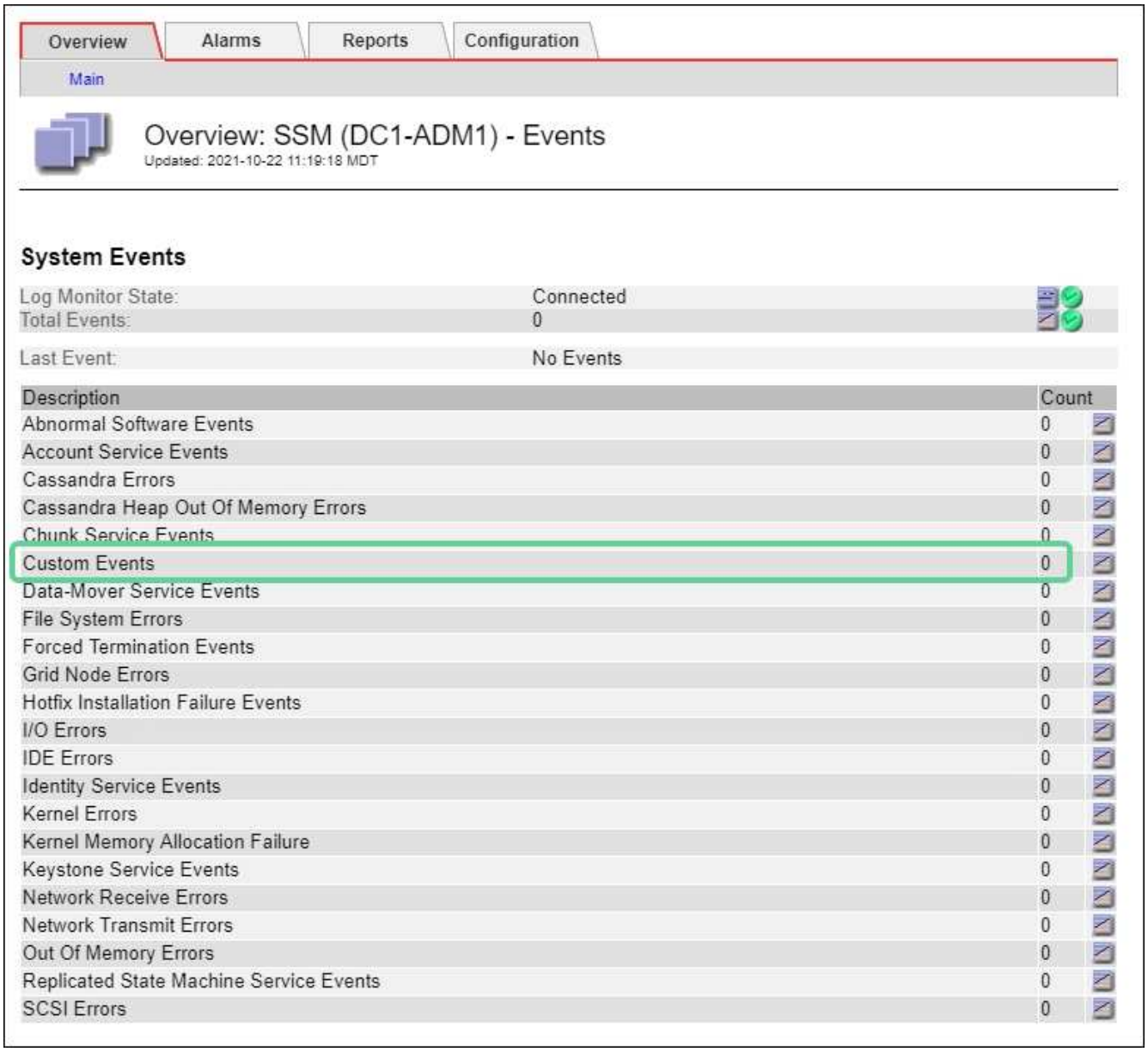
1. Selecione **SUPPORT** > **Alarmes (legacy)** > **Custom events**.

2. Clique em **Edit** (ou **Insert** se este não for o primeiro evento).
3. Introduza uma cadeia de eventos personalizada, por exemplo, encerramento



4. Selecione **aplicar alterações**.
5. Selecione **SUPPORT** > **Tools** > **Grid topology**.
6. Selecione ***grid node*** > **SSM** > **Eventos**.
7. Localize a entrada de Eventos personalizados na tabela Eventos e monitore o valor de **Count**.

   Se a contagem aumentar, um evento personalizado que você está monitorando está sendo acionado nesse nó de grade.



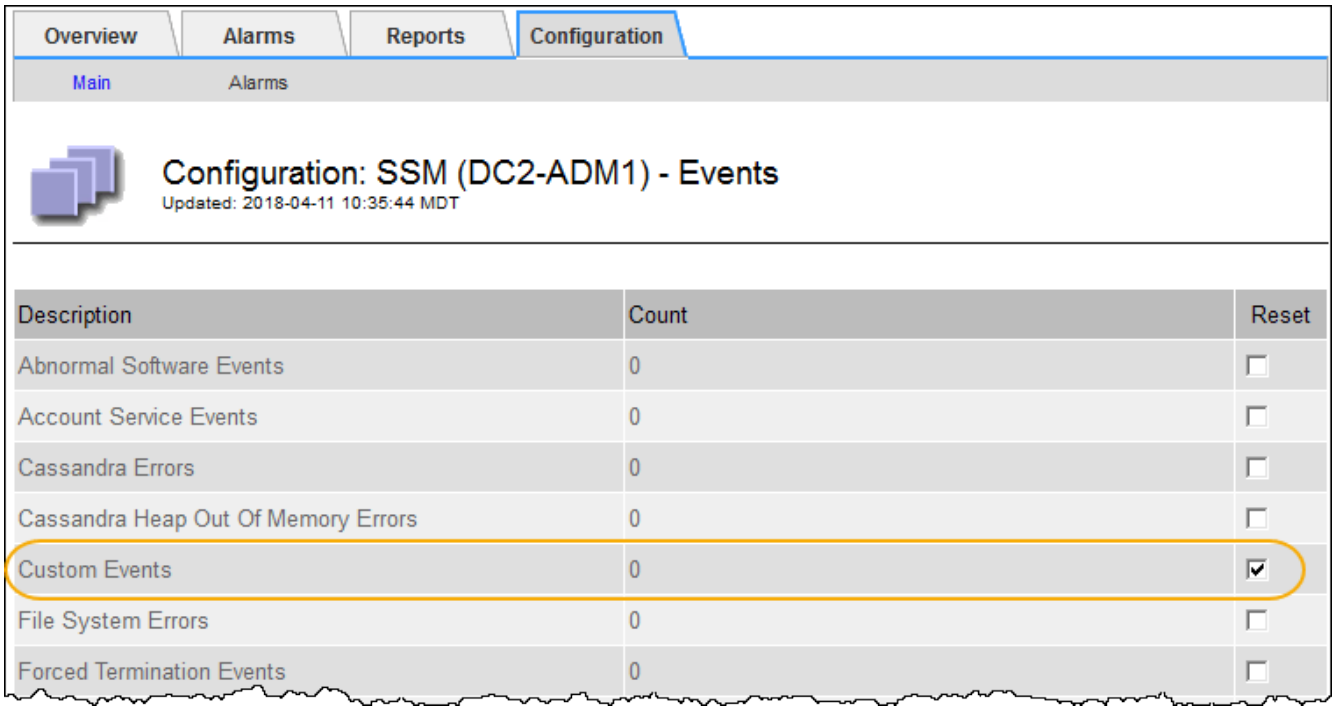
Redefina a contagem de eventos personalizados para zero

Se você quiser redefinir o contador apenas para eventos personalizados, use a página topologia de grade no menu suporte.

A reposição de um contador faz com que o alarme seja acionado pelo próximo evento. Em contraste, quando você reconhece um alarme, esse alarme só é reacionado se o próximo nível de limiar for atingido.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***grid node*** > **SSM** > **Eventos** > **Configuração** > **Principal**.
3. Marque a caixa de seleção **Reset** para Eventos personalizados.



4. Selecione **aplicar alterações**.

Rever mensagens de auditoria

As mensagens de auditoria podem ajudá-lo 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 StorageGRID geram mensagens de auditoria, como segue:

- 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 storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento de objetos e recuperações, 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 ou Swift faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento Registram solicitações de usuários para a API de gerenciamento.

Cada nó Admin armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compatados de dias anteriores. Cada nó na grade também armazena uma cópia das informações de auditoria geradas no nó.

Para facilitar o acesso aos logs de auditoria, você pode "Configurar acesso de cliente de auditoria para NFS". Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

O StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- O padrão do StorageGRID é destinos de auditoria de nó local.

- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de storage.
- 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 a ser 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, "Rever registos de auditoria"consulte .

Colete arquivos de log e dados do sistema

Você pode usar o Gerenciador de Grade para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade no nó Admin principal usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você deve ter a senha de provisionamento.

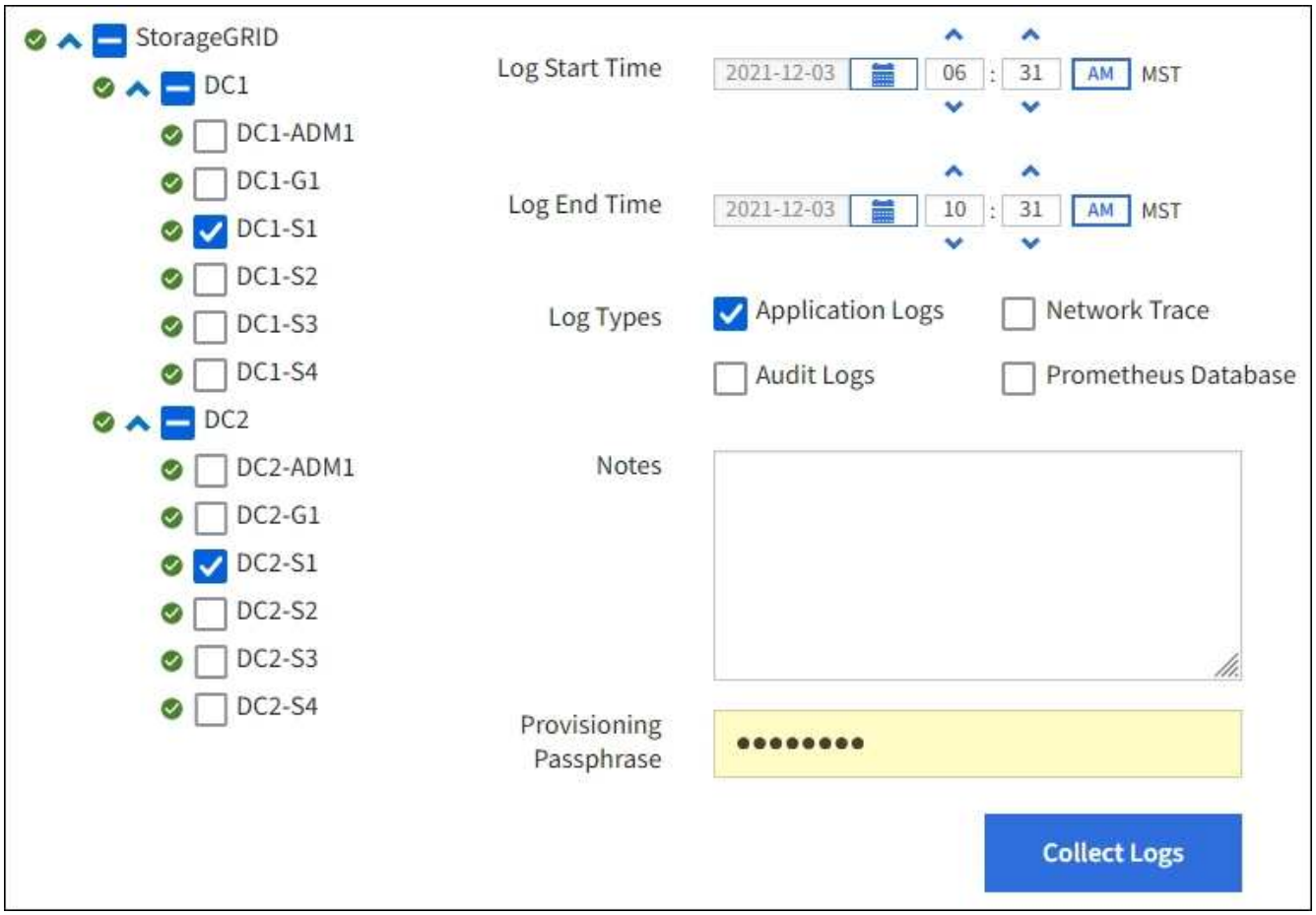
Sobre esta tarefa

Você pode usar o Gerenciador de Grade para coletar "ficheiros de registo", 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 a ser gerados e armazenados quando um servidor syslog externo é configurado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Passos

1. Selecione **SUPPORT** > **Tools** > **Logs**.



2. Selecione os nós de grade para os quais você deseja coletar arquivos de log.

   Conforme necessário, você pode coletar arquivos de log para toda a grade ou para todo o site do data center.

3. Selecione **hora de início** e **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 pode se tornar muito grande para ser armazenado em um nó ou muito grande para ser coletado para o nó de administração principal para download. Se isso ocorrer, você deve reiniciar a coleta de logs com um conjunto menor de dados.

4. Selecione os tipos de registos que pretende recolher.
   - **Logs de aplicativos**: Logs específicos de aplicativos que o suporte técnico utiliza com mais frequência para solução de problemas. Os registos recolhidos são um subconjunto dos registos de aplicações disponíveis.
   - **Logs de auditoria**: Logs contendo as mensagens de auditoria geradas durante a operação normal do sistema.
   - **Rastreamento de rede**: Logs usados para depuração de rede.
   - **Prometheus Database**: Métricas de séries temporais dos serviços em todos os nós.
5. Opcionalmente, insira notas sobre os arquivos de log que você está reunindo 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 anotações são adicionadas a um arquivo `info.txt` chamado ,

juntamente com outras informações sobre a coleção de arquivos de log. O `info.txt` ficheiro é guardado no pacote de arquivo de registo.

6. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.
7. Selecione **Collect 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 coleção de arquivos de log para cada nó de grade.

   Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo menor ou por menos nós.

8. Selecione **Download** quando a coleção de arquivos de log estiver concluída.

   O arquivo *.tar.gz* contém todos os arquivos de log de todos os nós de grade onde a coleta de log foi bem-sucedida. Dentro do arquivo combinado *.tar.gz*, há um arquivo de log para cada nó de grade.

Depois de terminar

Você pode baixar novamente o pacote de arquivo de log mais tarde, se precisar.

Opcionalmente, você pode selecionar **Excluir** para remover o pacote de arquivo de log e liberar espaço em disco. O pacote de arquivo de log atual é removido automaticamente da próxima vez que você coletar arquivos de log.

Acione manualmente um pacote AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente um pacote AutoSupport a ser enviado.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Na guia **ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** 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.

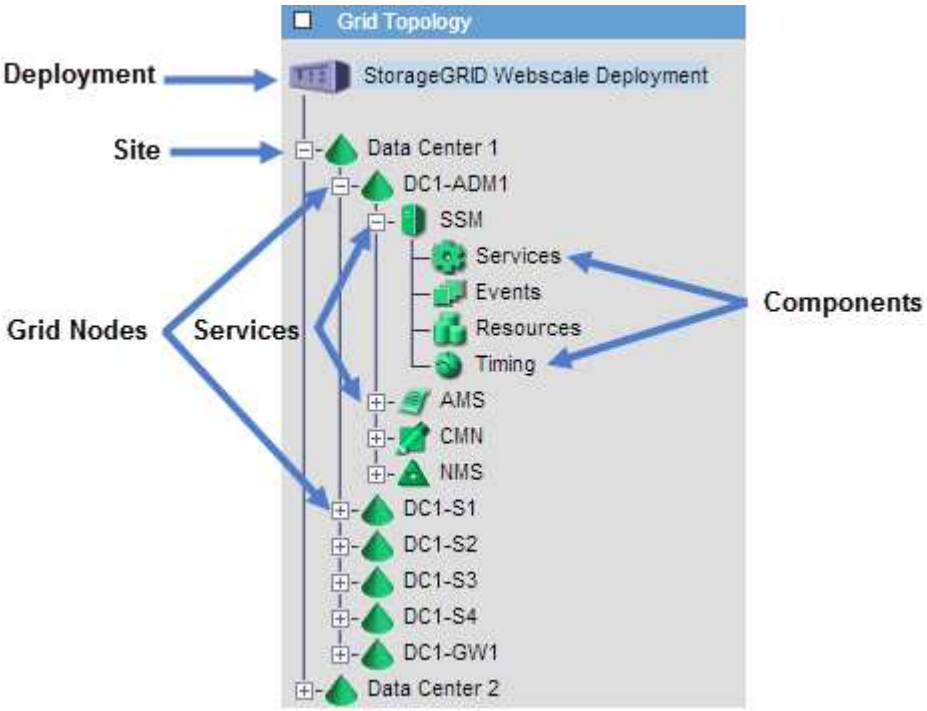
   > Depois de enviar um pacote AutoSupport acionado pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Veja a árvore de topologia de Grade

A árvore de topologia de grade fornece acesso a informações detalhadas sobre

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 quando estiver trabalhando com suporte técnico.

Para acessar a árvore de topologia de grade, selecione **SUPPORT** > **Tools** > **Grid topology**.



Para expandir ou recolher a árvore de topologia de Grade, clique ⊞ ou no local, nó ou ⊟ nível de serviço. Para expandir ou recolher todos os itens em todo o site ou em cada nó, mantenha pressionada a tecla **<Ctrl>** e clique em.

Atributos do StorageGRID

Atributos reportam valores e status para muitas das funções do sistema StorageGRID. Os valores de atributo estão disponíveis para cada nó de grade, cada local e toda a grade.

Os atributos do StorageGRID são usados em vários lugares no Gerenciador de Grade:

- **Página de nós**: Muitos dos valores mostrados na página de nós são atributos StorageGRID. (As métricas Prometheus também são mostradas nas páginas de nós.)
- **Alarmes**: Quando os atributos atingem valores de limite definidos, os alarmes StorageGRID (sistema legado) são acionados em níveis de gravidade específicos.
- **Grid Topology tree**: Os valores de atributo são mostrados na árvore Grid Topology (**SUPPORT** > **Tools** > **Grid topology**).
- **Eventos**: Os eventos do sistema ocorrem quando certos atributos Registram uma condição de erro ou falha para um nó, incluindo erros como erros de rede.

Valores de atributo

Os atributos são reportados com o 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, os atrasos de propagação podem retardar o relatório de atributos. Os valores atualizados para a maioria dos atributos são enviados para o sistema StorageGRID em intervalos fixos. Pode demorar vários minutos até que uma atualização seja visível no sistema, e dois atributos que mudam mais ou menos simultaneamente podem ser reportados em momentos ligeiramente diferentes.

Analise as métricas de suporte

Ao solucionar um problema, você pode trabalhar com suporte técnico para analisar métricas e gráficos detalhados do seu sistema StorageGRID.

Antes de começar

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

Sobre esta tarefa

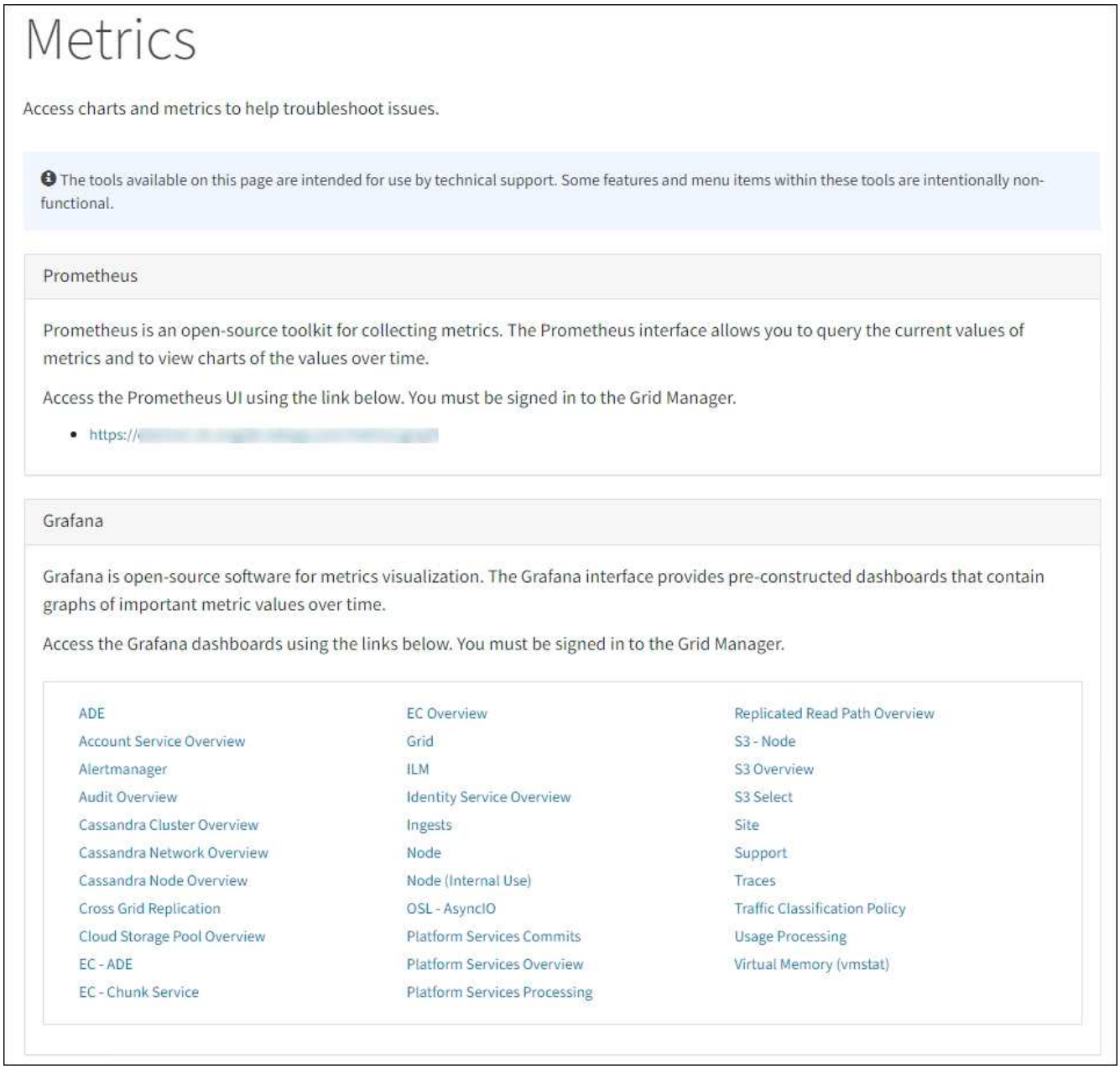
A página Metrics permite que você acesse as interfaces de usuário Prometheus e Grafana. Prometheus é um software de código aberto para coletar métricas. Grafana é um software de código aberto para visualização de métricas.

> ⓘ As ferramentas disponíveis na página Metrics destinam-se a ser utilizadas pelo suporte técnico. Alguns recursos e itens de menu dentro dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Consulte a lista "Métricas de Prometheus comumente usadas"de .

Passos

1. Conforme indicado pelo suporte técnico, selecione **SUPPORT** > **Tools** > **Metrics**.

   Um exemplo da página Metrics 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 Prometheus é exibida. Você pode usar essa interface para executar consultas sobre as métricas disponíveis do StorageGRID e para traçar métricas do StorageGRID ao longo do tempo.

   > As 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 Grafana para o link selecionado é exibida.

Execute o diagnóstico

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no sistema StorageGRID e analisar os resultados.

- "Analise as métricas de suporte"
- "Métricas de Prometheus comumente usadas"

Antes de começar

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

Sobre esta tarefa

A página Diagnósticos executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um de três Estados:

-

- **Normal**: Todos os valores estão dentro do intervalo normal.
- **Atenção**: Um ou mais valores estão fora do intervalo normal.
- **Atenção**: Um ou mais dos valores estão significativamente fora do intervalo normal.

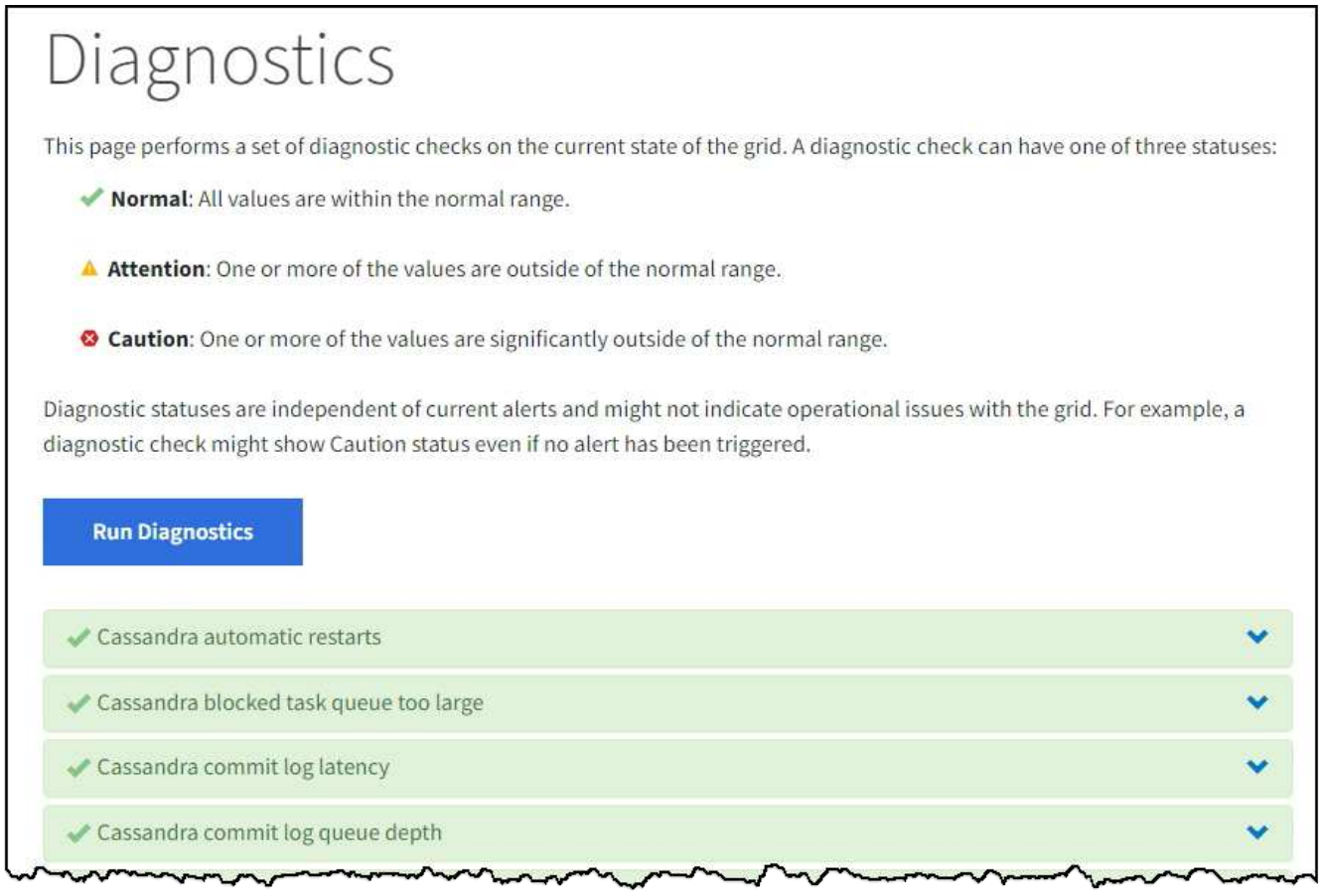
Os Estados de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a grade. Por exemplo, uma verificação de diagnóstico pode mostrar o estado de precaução mesmo que nenhum alerta tenha sido acionado.

Passos

1. Selecione **SUPPORT** > **Tools** > **Diagnostics**.

   A página Diagnósticos é exibida e lista os resultados de cada verificação de diagnóstico. Os resultados são classificados por gravidade (cuidado, atenção e, em seguida, normal). Dentro de cada gravidade, os resultados são ordenados alfabeticamente.

   Neste exemplo, todos os diagnósticos têm um estado normal.



2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

   São apresentados detalhes sobre o diagnóstico e os seus resultados atuais. Os seguintes detalhes são listados:

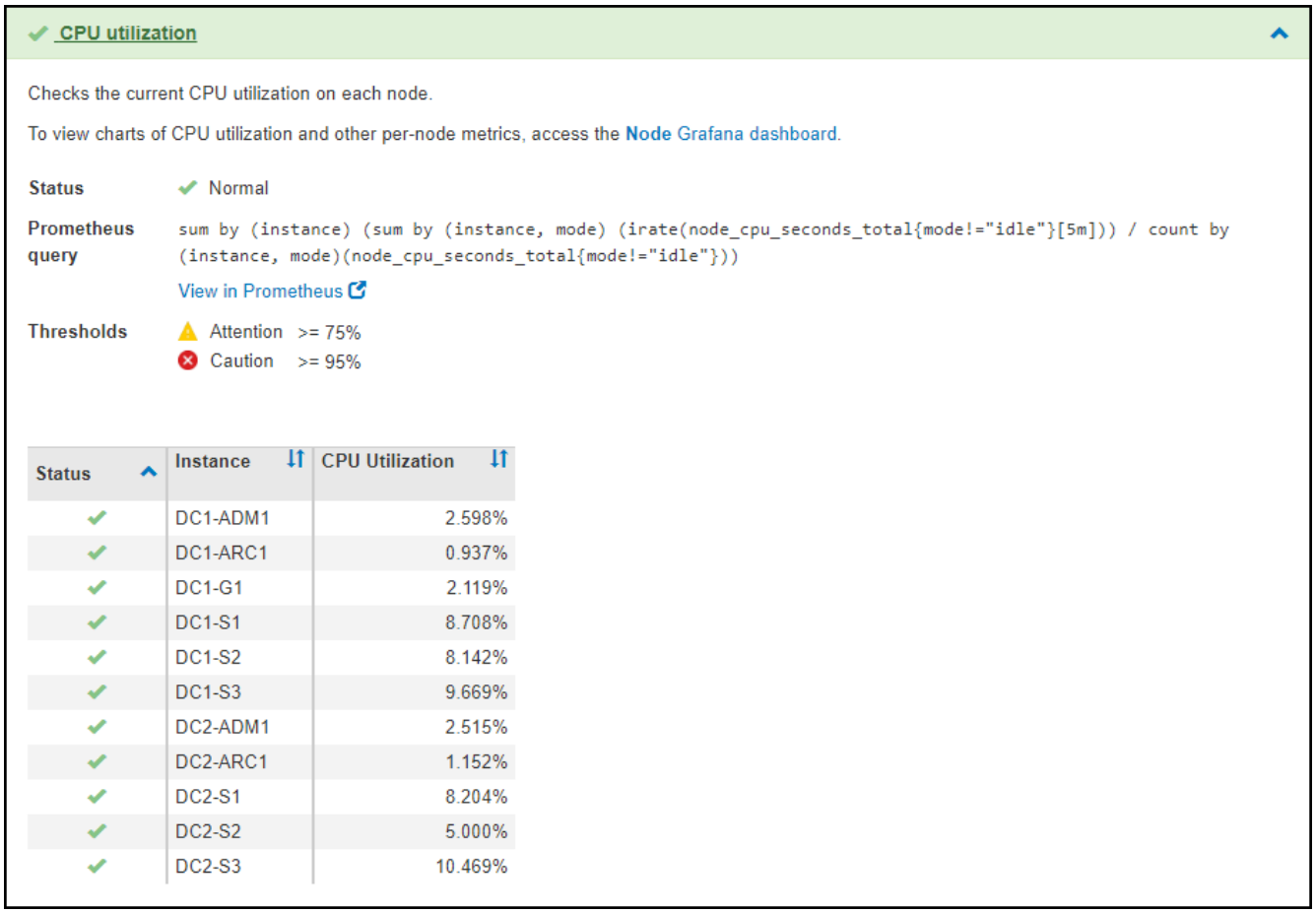
   - **Status**: O estado atual deste diagnóstico: Normal, atenção ou cuidado.
   - **Consulta Prometheus**: Se usada para o diagnóstico, a expressão Prometheus que foi usada para

gerar os valores de status. (Uma expressão Prometheus não é usada para todos os diagnósticos.)

- **Limiares**: Se disponíveis para o diagnóstico, os limiares definidos pelo sistema para cada estado de diagnóstico anormal. (Os valores de limite não são usados para todos os diagnósticos.)

  Não é possível alterar esses limites.

- **Valores de estado**: Uma tabela que mostra o estado e o valor do diagnóstico em todo o sistema StorageGRID. Neste exemplo, a utilização atual da CPU para cada nó em um sistema StorageGRID é mostrada. Todos os valores de 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**.

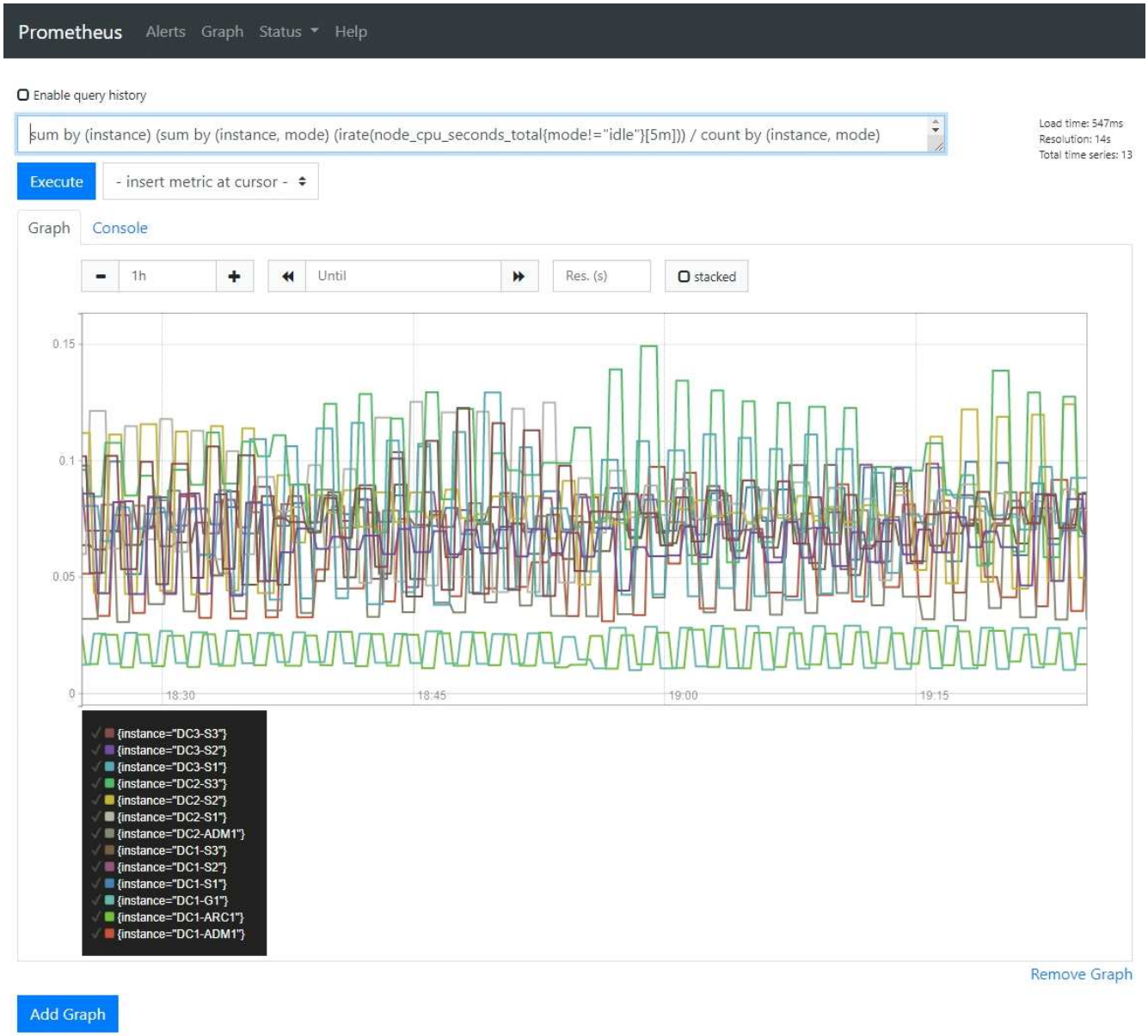
   Este link não é exibido para todos os diagnósticos.

   O painel do Grafana relacionado é exibido. Neste exemplo, o painel Node aparece mostrando a utilização da CPU ao longo do tempo para este nó, bem como outros gráficos Grafana para o nó.

   Você também pode acessar os painéis Grafana pré-construídos na seção Grafana da página **SUPPORT** > **Tools** > **Metrics**.

4. **Opcional**: Para ver um gráfico da expressão Prometheus ao longo do tempo, clique em **Exibir em Prometheus**.

   Aparece um gráfico Prometheus da expressão usada no diagnóstico.



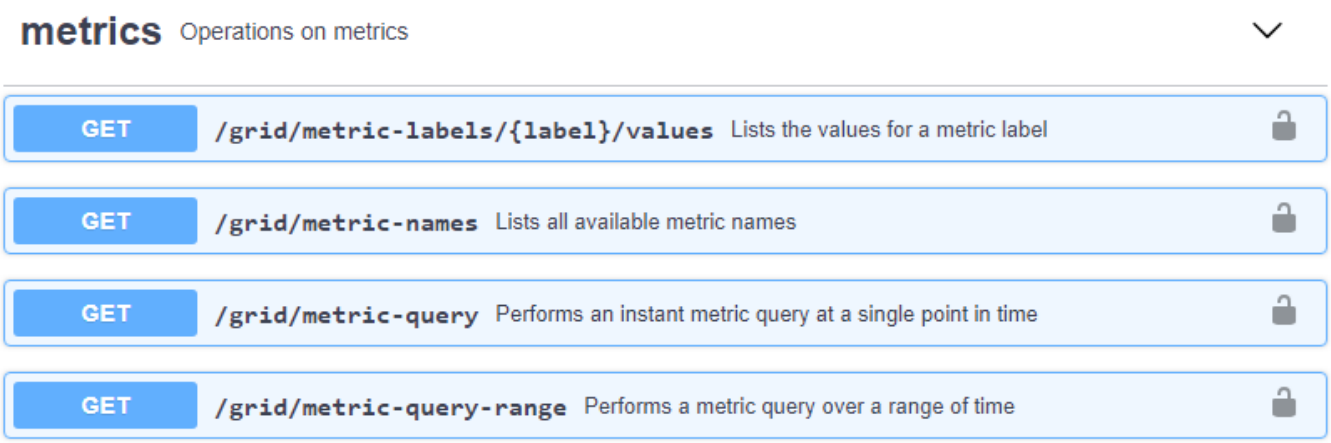
Crie aplicativos de monitoramento personalizados

Você pode criar aplicativos e painéis de monitoramento 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 Gerenciador de Grade ou se quiser criar painéis personalizados para o StorageGRID, use a API de Gerenciamento de Grade para consultar métricas do StorageGRID.

Você também pode acessar métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como Grafana. O uso de uma ferramenta externa requer que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Consulte "Instruções para administrar o StorageGRID".

Para exibir as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Gerenciador de Grade. Na parte superior 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: Visão geral

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

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

defina o problema

O primeiro passo para resolver um problema é definir o problema claramente.

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

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não está fazendo? Quais são seus sintomas?	Os aplicativos clientes estão relatando que os objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez em cerca de 14:50 em 8 de janeiro de 2020.
Como você notou o problema pela primeira vez?	Notificado pela aplicação do cliente. Também recebeu notificações por e-mail de alerta.
O problema acontece de forma consistente, ou apenas às vezes?	O problema está em curso.
Se o problema ocorrer regularmente, quais as etapas que o causam	O problema acontece toda vez que um cliente tenta ingerir um objeto.

Pergunta	Exemplo de resposta
Se o problema ocorrer intermitentemente, quando ocorre? Registre os horários de cada incidente que você está ciente.	O problema não é intermitente.
Você já viu esse problema antes? Com que frequência você teve esse problema no passado?	Esta é a primeira vez que vi esta questão.

Avaliar o risco e o impactos no sistema

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

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

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

Coletar dados

Depois de definir o problema e avaliar o seu risco e impactos, recolha dados para análise. O tipo de dados que é mais útil para coletar depende da natureza do problema.

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Crie a linha do tempo das mudanças recentes	As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.	• Crie uma linha do tempo das mudanças recentes

Tipo de dados a recolher	Por que coletar esses dados	Instruções
Reveja alertas e alarmes	Alertas e alarmes podem ajudá-lo a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso. Revise a lista de alertas e alarmes atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Reveja alertas e alarmes acionados no passado para obter informações adicionais.	• "Ver alertas atuais e resolvidos" • "Gerenciar alarmes (sistema legado)"
Monitorar eventos	Os eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas apareceram pela primeira vez e podem ajudá-lo a entender a rapidez com que as coisas estão mudando.	• "Use gráficos e gráficos" • "Use relatórios de texto"
Estabeleça linhas de base	Recolher informações sobre os níveis normais de vários valores operacionais. Esses valores de linha de base, e desvios dessas linhas de base, podem fornecer pistas valiosas.	• Estabeleça linhas de base
Execute testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com os vistos ao usar o aplicativo cliente.	• "Monitore O PUT e obtenha desempenho"
Rever mensagens de auditoria	Revise as mensagens de auditoria para seguir as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Rever mensagens de auditoria"
Verifique os locais dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de storage.	• "Monitorar operações de verificação de objetos" • "Confirmar localizações de dados do objeto" • "Verifique a integridade do objeto"

Tipo de dados a recolher	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.	• "Colete arquivos de log e dados do sistema" • "Acione manualmente um pacote AutoSupport" • "Analise as métricas de suporte"

Crie uma linha do tempo de mudanças recentes

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

- As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.
- Uma linha do tempo de mudanças pode ajudá-lo a identificar quais mudanças podem ser responsáveis por um problema e como cada mudança pode ter afetado seu desenvolvimento.

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

Hora da mudança	Tipo de alteração	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização de software foi concluída? • Interrompeu o processo?	O que aconteceu? O que fez?	Documente todos os detalhes relevantes sobre a alteração. Por exemplo: • Detalhes das alterações de rede. • Qual hotfix foi instalado. • Como as cargas de trabalho do cliente mudaram. Certifique-se de observar se mais de uma mudança estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi recentemente instalado, expandido ou recuperado?
- O sistema foi atualizado recentemente? Foi aplicado um hotfix?
- Algum hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?

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

Estabeleça linhas de base

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

Propriedade	Valor	Como obter
Consumo médio de storage	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - dados do objeto, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar a quantidade de armazenamento consumida a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.

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

Propriedade	Valor	Como obter
Latência média da consulta	Milissegundos	Selecione **NODES** > ***Storage Node*** > **Objects**. Na tabela consultas, exiba o valor da latência média.

Analisar dados

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

A análise é dependente de problemas, mas em geral:

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

Lista de verificação de informações de encaminhamento

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

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, que horas ocorreu? Defina o problema
	Avaliação de impactos	Qual é a gravidade do problema? Qual é o impactos na aplicação cliente? • O cliente foi conetado com sucesso antes? • O cliente pode obter, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione **MAINTENANCE** > **System** > **License**. A ID do sistema StorageGRID é apresentada como parte da licença atual.
	Versão do software	Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **sobre** para ver a versão do StorageGRID.

✔	Item	Notas
	Personalização	Resumir como o seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grade usa compactação de storage, criptografia de storage ou conformidade? • O ILM faz objetos replicados ou codificados por apagamento? O ILM garante a redundância do site? As regras do ILM usam os comportamentos de ingestão equilibrada, rigorosa ou dupla confirmação?
	Ficheiros de registo e dados do sistema	Recolha ficheiros de registo e dados do sistema para o seu sistema. Selecione **SUPPORT** > **Tools** > **Logs**. Você pode coletar logs para toda a grade ou para nós selecionados. Se você estiver coletando logs somente para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de storage em um local incluem o serviço ADC.) "Colete arquivos de log e dados do sistema"
	Informações da linha de base	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabeleça linhas de base
	Cronograma das mudanças recentes	Crie uma linha do tempo que resume quaisquer alterações recentes ao sistema ou ao 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, certifique-se de Registrar as etapas que você tomou e o resultado.

Solucionar problemas de objetos e storage

Confirmar localizações de dados do objeto

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

Antes de começar

- Você deve ter um identificador de objeto, que pode ser um dos seguintes:

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

Passos

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

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

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

4. Selecione **Procurar**.

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

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

liberação para liberação.

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Falhas no armazenamento de objetos (volume de storage)

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

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

Disk devices

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

Volumes

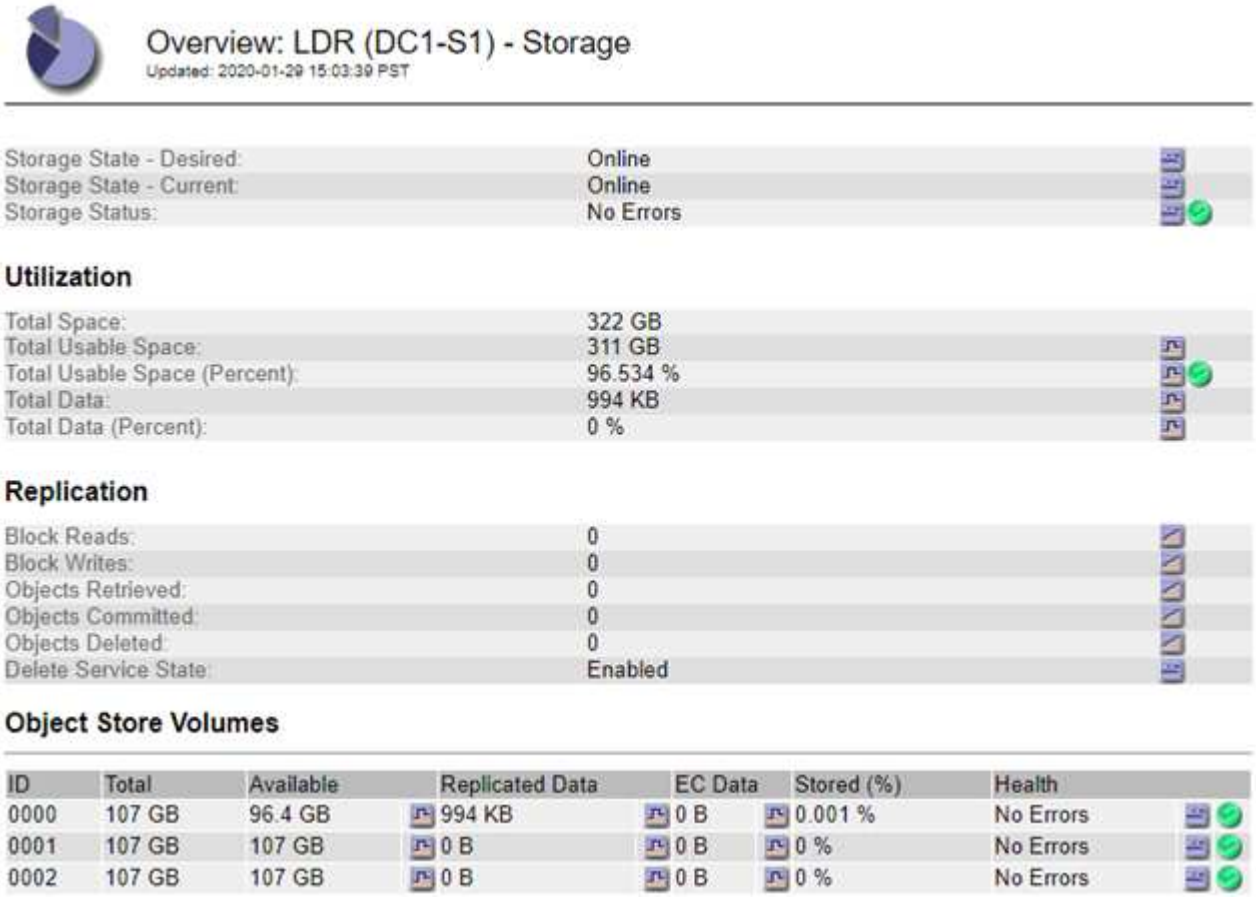
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

Object stores

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

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

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



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

Verifique a integridade do objeto

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

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

O que é a verificação em segundo plano?

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

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

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

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

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

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

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

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

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

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

Altere a taxa de verificação em segundo plano

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

Antes de começar

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

Sobre esta tarefa

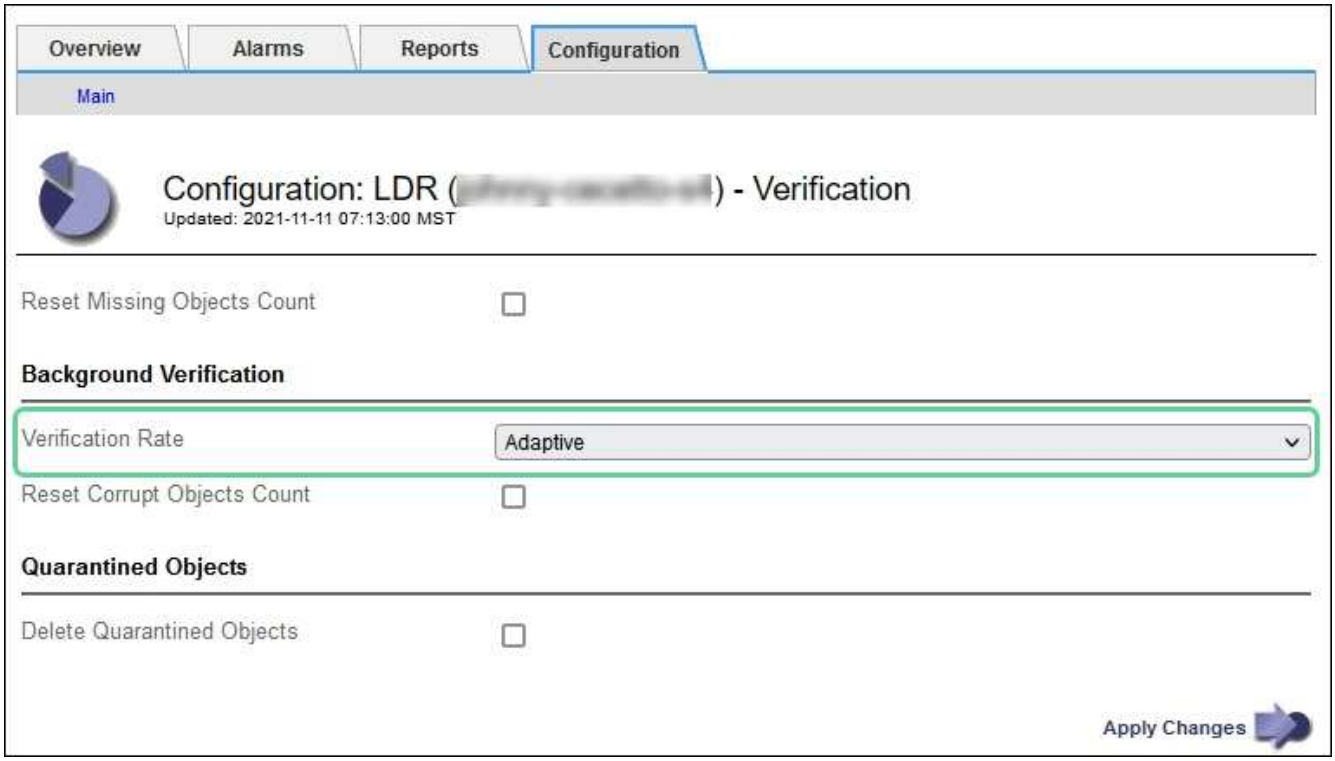
Você pode alterar a taxa de verificação para verificação em segundo plano em um nó de storage:

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

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

Passos

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



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

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

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

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

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

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

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

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

9. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID, redefina a contagem de objetos corrompidos.
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***Storage Node*** > **LDR** > **Verificação** > **Configuração**.
   c. Selecione **Redefinir contagem de objetos corrompidos**.
   d. Clique em **aplicar alterações**.

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

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

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

O que é verificação de existência de objeto?

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

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

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

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

Executar verificação de existência de objeto

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

Antes de começar

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

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

Sobre esta tarefa

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

Passos

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

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

   Você pode pesquisar por nome do nó ou site.

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

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

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

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

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

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

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

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

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

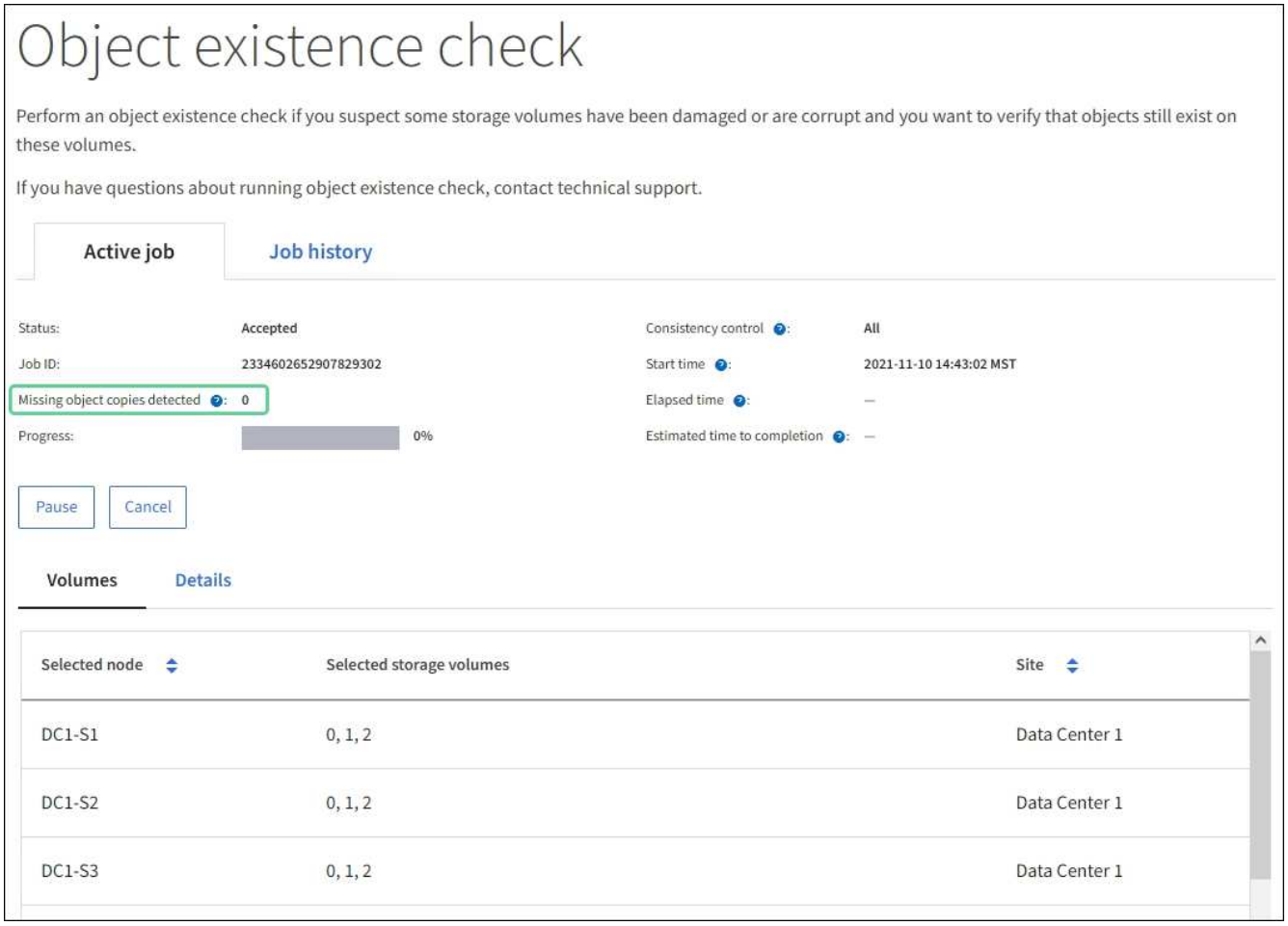
   - O trabalho é concluído.
   - Pausa ou cancelar o trabalho. Você pode retomar um trabalho em pausa, mas não pode retomar um trabalho cancelado.
   - O trabalho vai abaixo. O alerta **Object existence check has stalled** é acionado. Siga as ações corretivas especificadas para o alerta.
   - O trabalho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

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

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

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

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



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

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

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

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

perdidas.

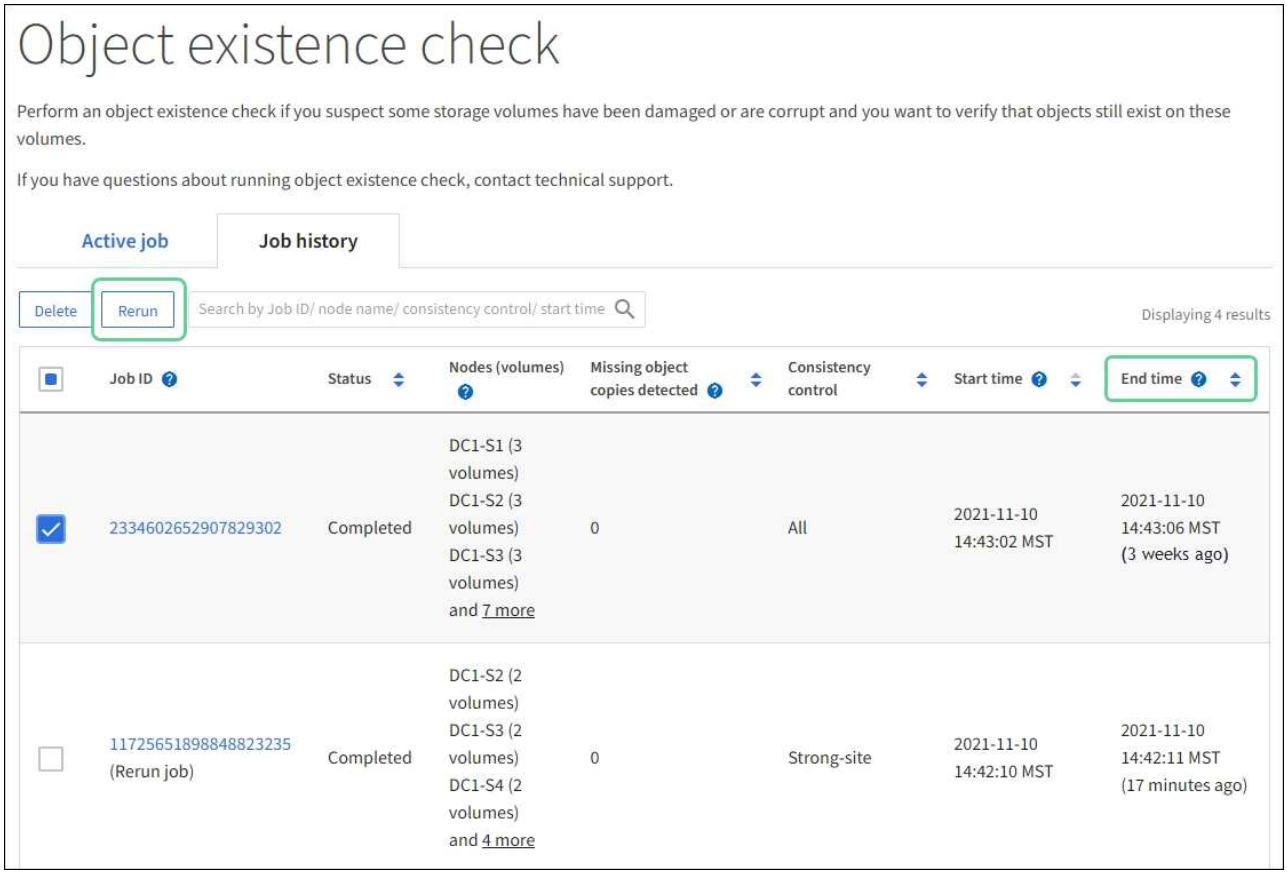
a. Selecione **MAINTENANCE** > **Object existence check** > **Job history**.

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

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

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

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



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

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

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

Depois de terminar

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

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

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

Antes de começar

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

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

Passos

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

   a. Introduza `ssh admin@primary_Admin_Node_IP`

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

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

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

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

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

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

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

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

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

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

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

      ii. Para cada mensagem de auditoria nos resultados, observe `S3AI` o campo para determinar o ID da

conta do locatário. Use os outros campos da mensagem para determinar qual endereço IP foi usado pelo cliente, pelo bucket e pelo objeto:

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

Exemplo de resultados de log de auditoria

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

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

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

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

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

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

      Exemplo bycast.log

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

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

Solucionar problemas de dados de objetos perdidos e ausentes

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

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

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

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

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

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

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

Investigue objetos perdidos

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

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

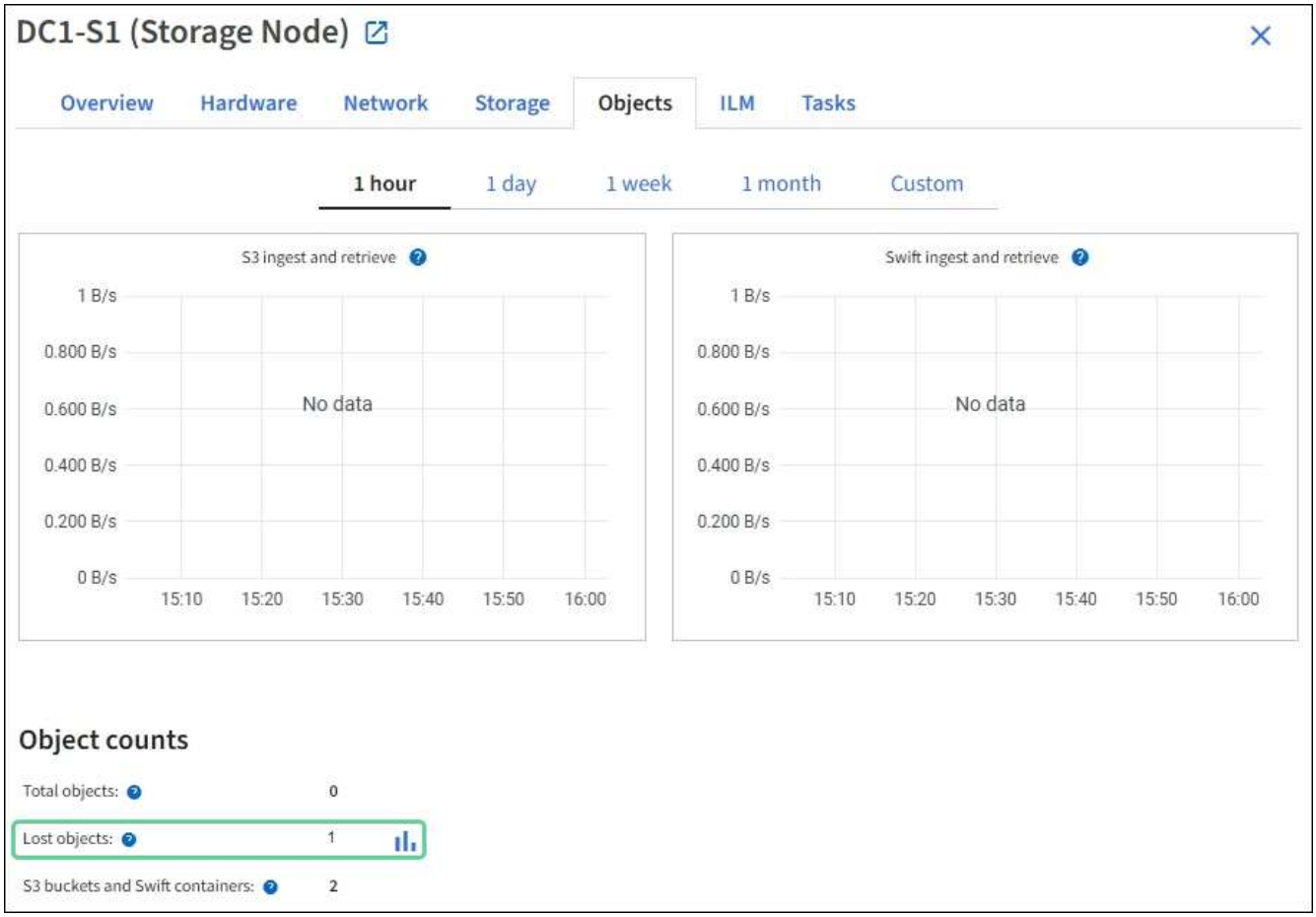
O alerta **objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

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

Passos

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

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



4. A partir de um nó Admin, "acesse o log de auditoria"para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **objetos perdidos**:
   a. Faça login no nó da grade:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
   b. Mude para o diretório onde os logs de auditoria estão localizados.

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

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

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

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

c. Use grep para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`

d. Observe o valor UUID incluído na mensagem.

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

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

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

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

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

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

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
```

```
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
```

```
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

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

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

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

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

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

Procure e restaure objetos potencialmente perdidos

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

Antes de começar

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

Sobre esta tarefa

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

Contacte o suporte técnico para obter assistência com este procedimento.

Passos

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

   a. Faça login no nó da grade:

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

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

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

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

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

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

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

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

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

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

      Por exemplo:

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

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

      Por exemplo:

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

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

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

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

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

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

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

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

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

a. Faça login no nó da grade:

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

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

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

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

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

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

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

Por exemplo, digite:

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

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

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

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

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

      Por exemplo, digite:

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

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

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

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

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

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

        Avance para o passo seguinte.

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

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

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

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

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

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

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

   a. Faça login no nó da grade:

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

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

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

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

   b. Mude para o diretório onde os logs de auditoria estão localizados. subetapa 1. bConsulte a .

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

      Por exemplo:

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

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

      Por exemplo:

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

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

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

a. Localize o campo LOCS na mensagem de auditoria.

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

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

Repor contagens de objetos perdidas e em falta

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

Antes de começar

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

Sobre esta tarefa

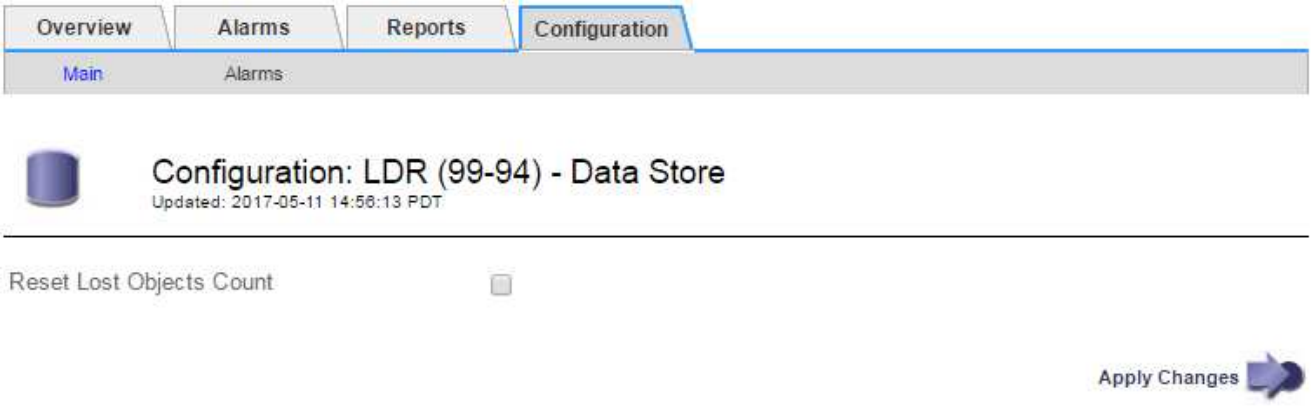
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

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

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

Passos

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



4. Clique em **aplicar alterações**.

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

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

   a. Selecione ***Site*** > ***Storage Node*** > **LDR** > **Codificação de apagamento** > **Configuração**.

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

   c. Clique em **aplicar alterações**.

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

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

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

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

   g. Clique em **aplicar alterações**.

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

Solucionar problemas do alerta de armazenamento de dados de objetos baixos

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Nesta condição:

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

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

Passos

1. Selecione **ALERTAS** > **atual**.

   A página Alertas é exibida.

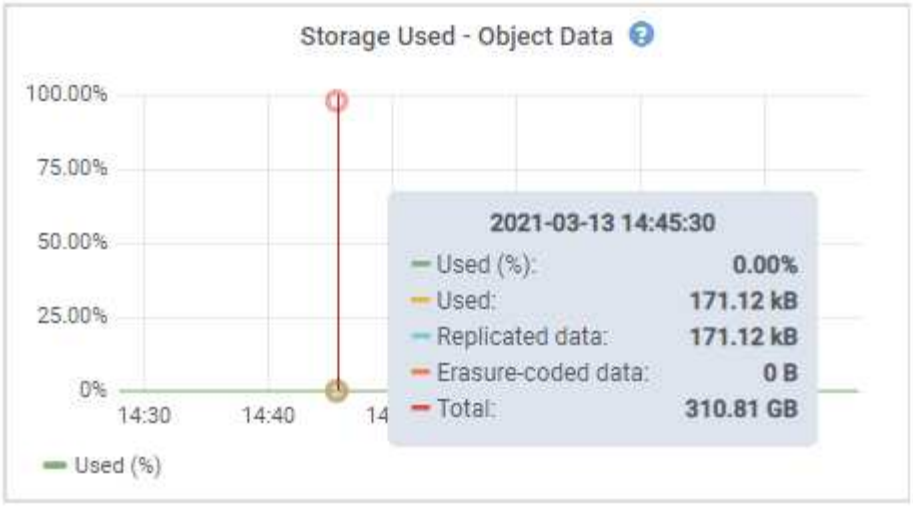
2. Na tabela de alertas, expanda o grupo de alertas **armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja exibir.

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

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

   São apresentados os seguintes valores:

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



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

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

7. Assim que possível, "adicionar capacidade de armazenamento" para a sua grade.

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

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

Informações relacionadas

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

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

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

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

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

- Seu sistema está próximo da capacidade e não poderá aceitar novos dados se forem aplicadas marcas de água otimizadas. Neste caso, o StorageGRID não alterará as configurações de marca d'água.

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

Entenda o alerta

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

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

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

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

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

Resolva o alerta

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

Antes de começar

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

Sobre esta tarefa

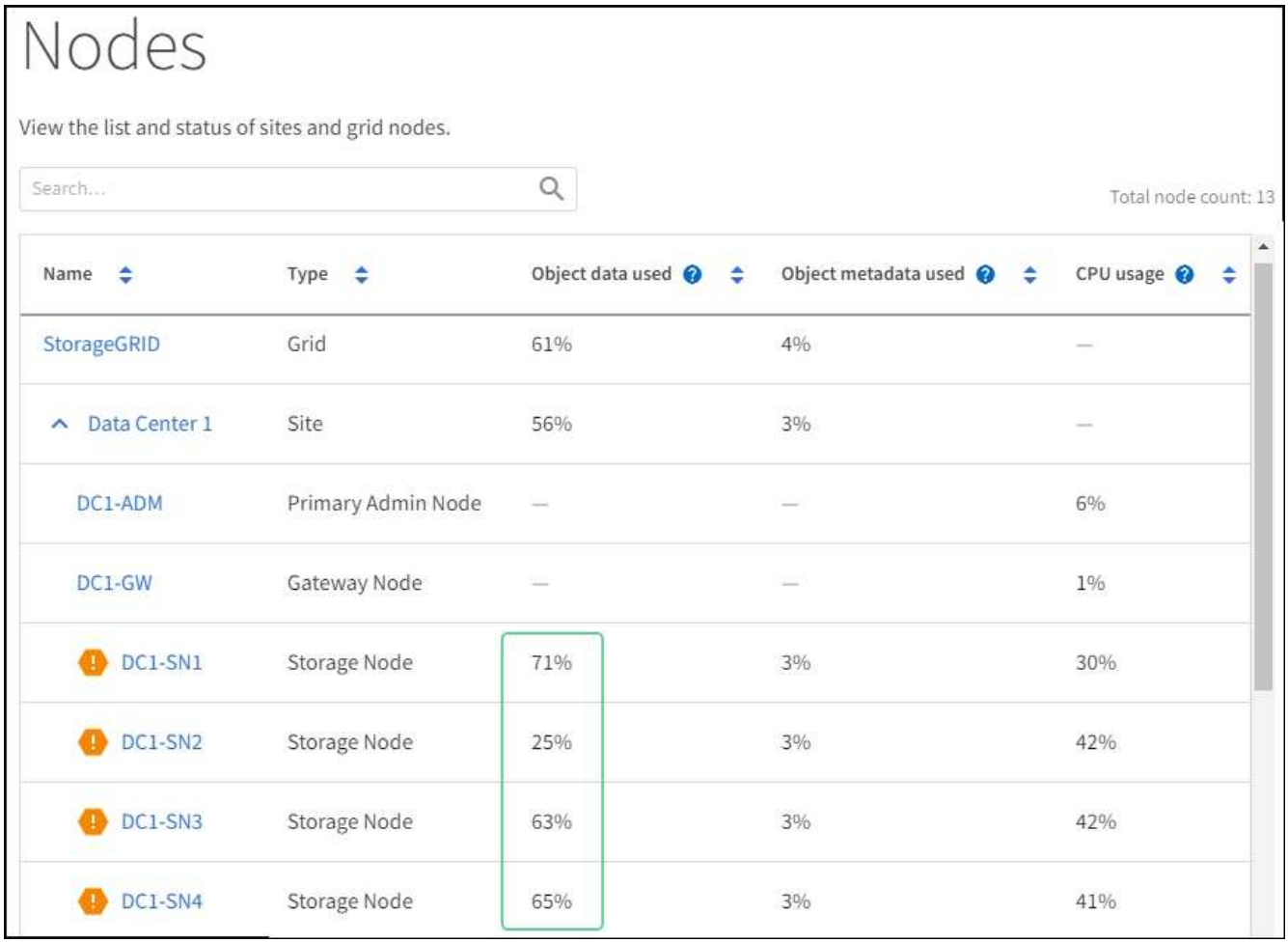
Você pode resolver o alerta * baixa substituição de marca d'água somente leitura * atualizando as configurações personalizadas de marca d'água para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem próximos do cheio ou se você tiver requisitos especiais de ILM,

primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados de objeto para toda a grade

Passos

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



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

Ver marcas de água de armazenamento otimizadas

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

máximo para cada nó de storage em sua grade.

Passos

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

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

determine se você pode usar marcas de água otimizadas

Passos

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

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

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

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

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

Passos

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

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

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

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

Antes de começar

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

Sobre esta tarefa

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

Storage Options Overview

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

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

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

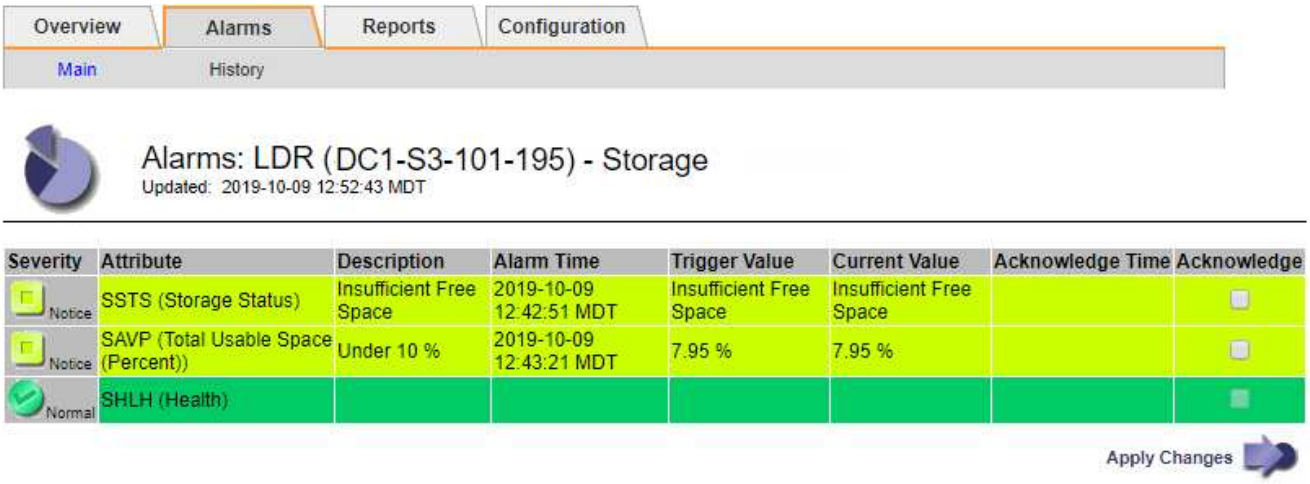
Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. O alarme SSTS é acionado se menos de 10 GB de espaço utilizável permanecer em cada volume de armazenamento no nó de armazenamento. Se algum dos volumes tiver 10 GB ou mais de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

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

Passos

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

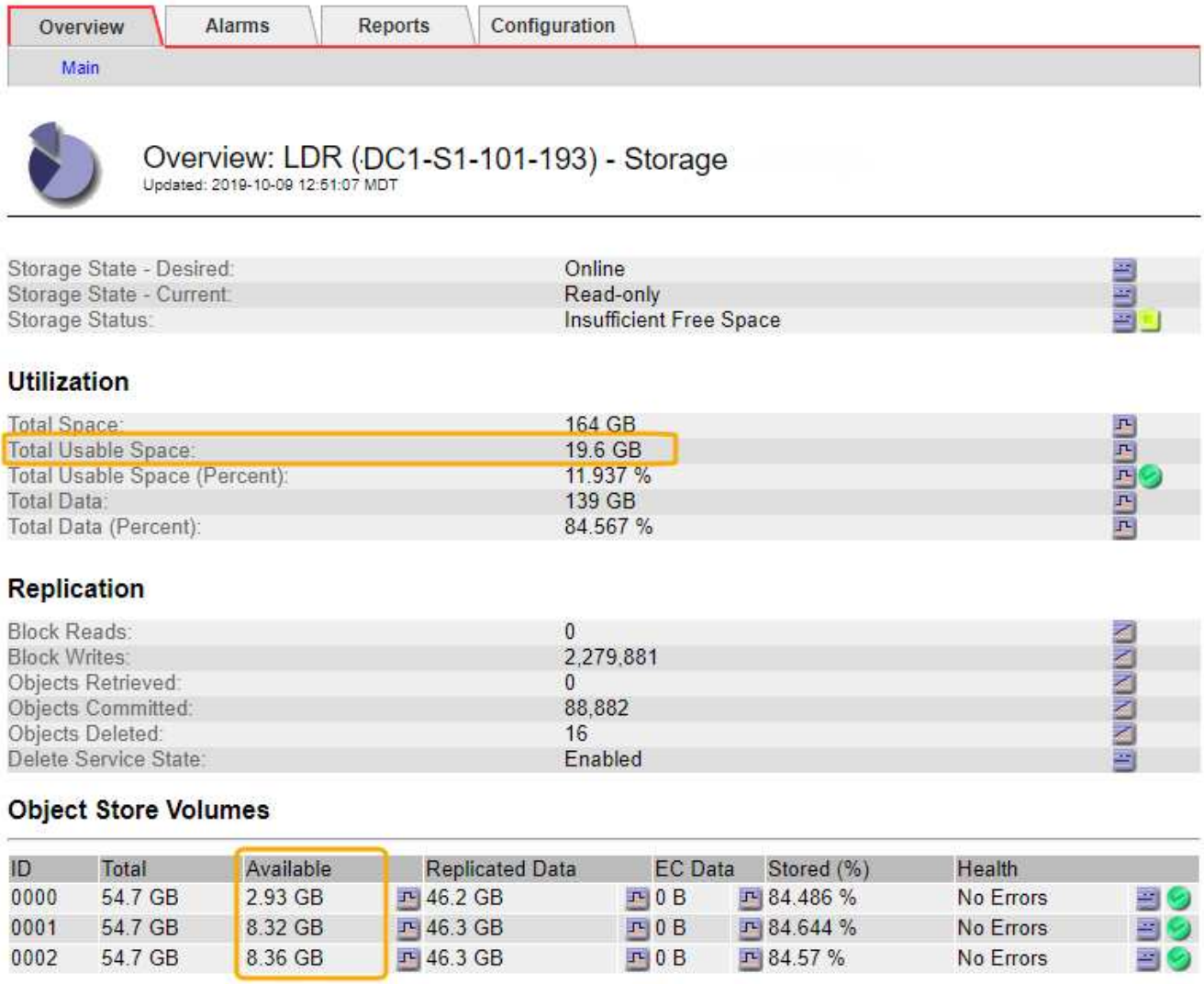
   É apresentada a página Grid Topology (topologia de grelha). A guia Alarmes mostra os alarmes ativos para o nó e serviço selecionados.



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

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

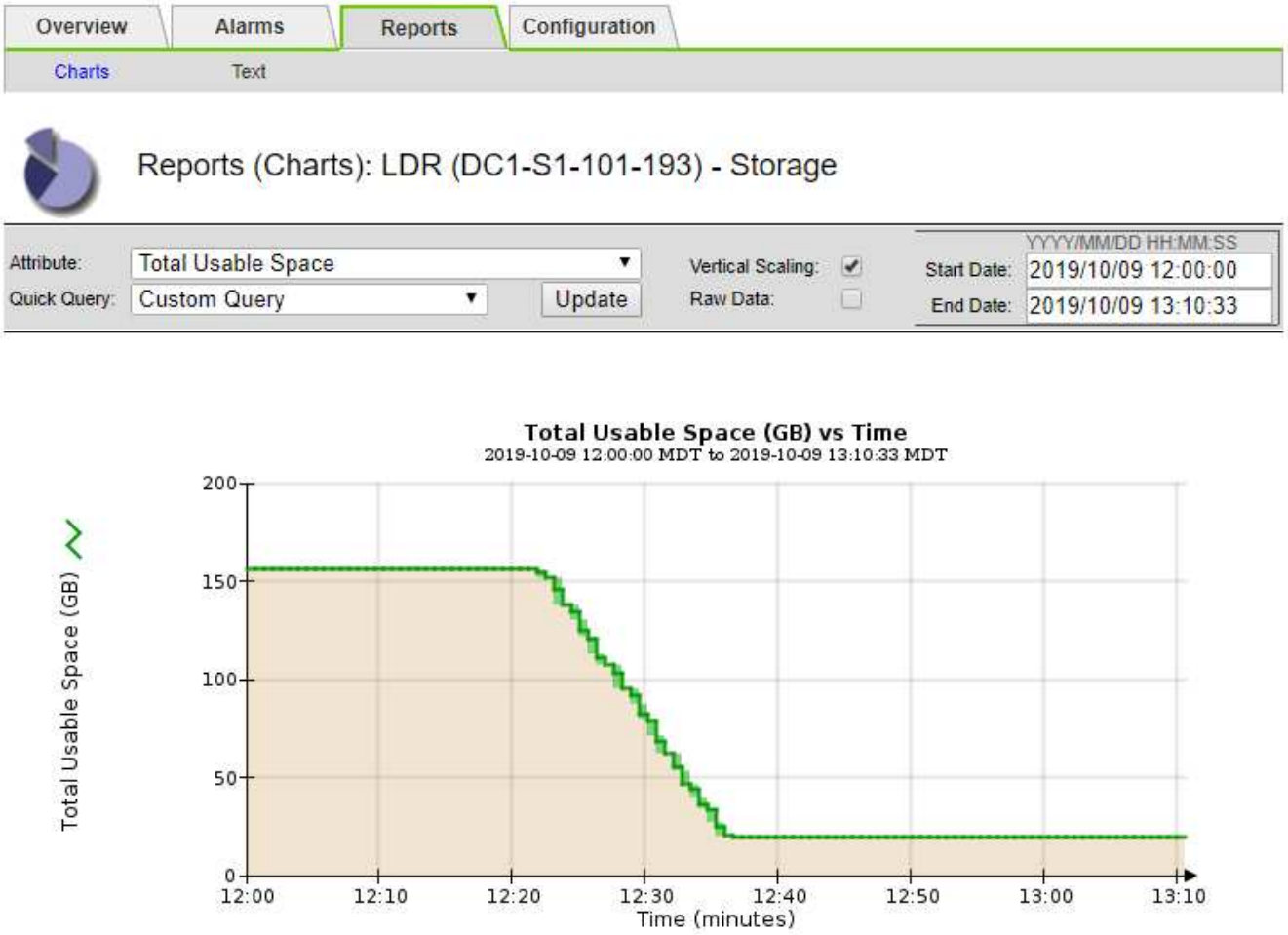
3. Para determinar quanto espaço utilizável está realmente disponível, selecione **LDR** > **Storage** > **Overview** e encontre o atributo espaço utilizável total (STAS).



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

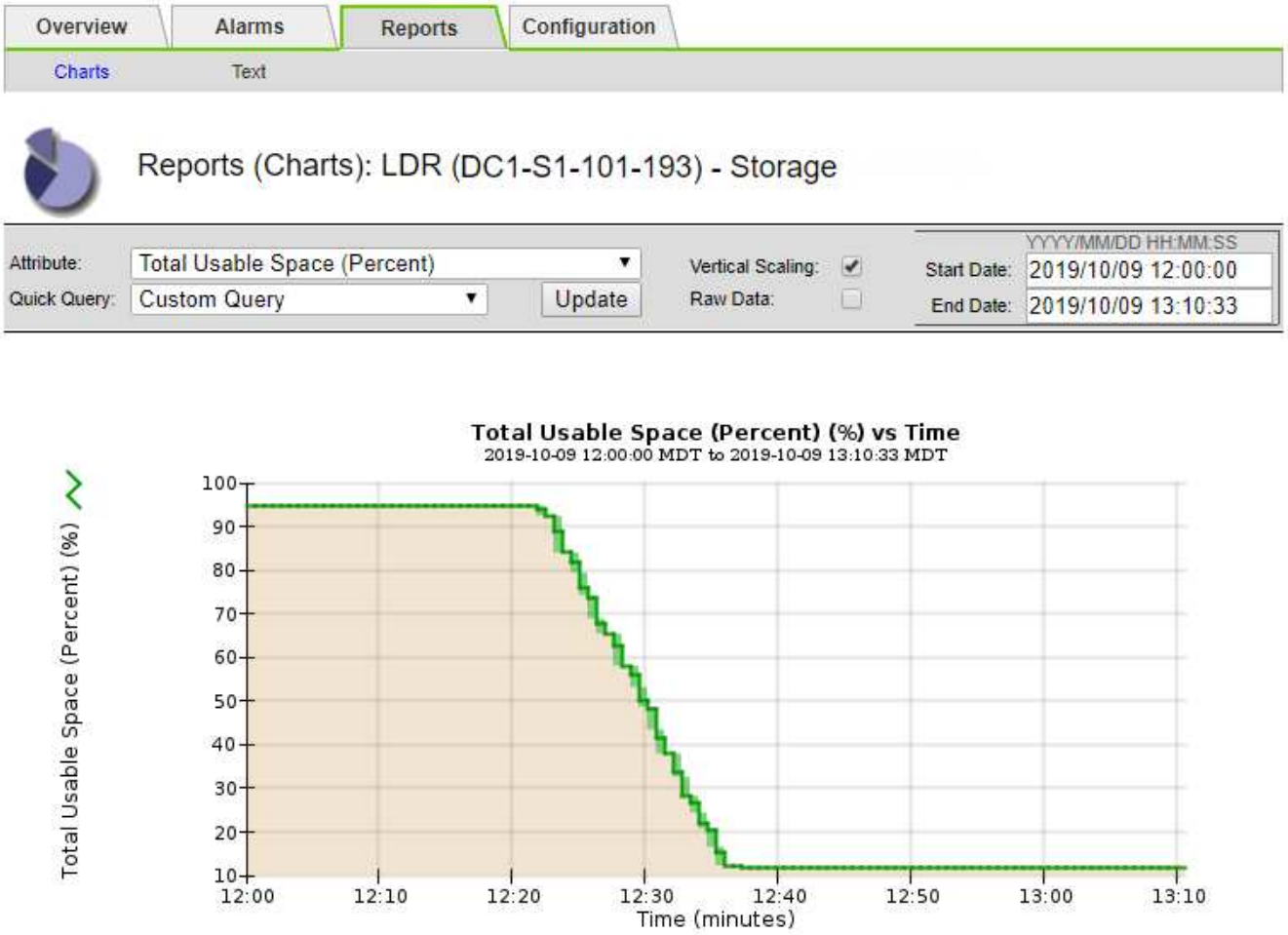
4. Para entender como o armazenamento foi usado ao longo do tempo, selecione a guia **relatórios** e plote o espaço utilizável total nas últimas horas.

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



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

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



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

   Consulte também "Gerencie nós de storage completos".

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

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

Sobre esta tarefa

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

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

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

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

Passos

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

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

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

Solucionar problemas de metadados

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

Alerta baixo de armazenamento de metadados

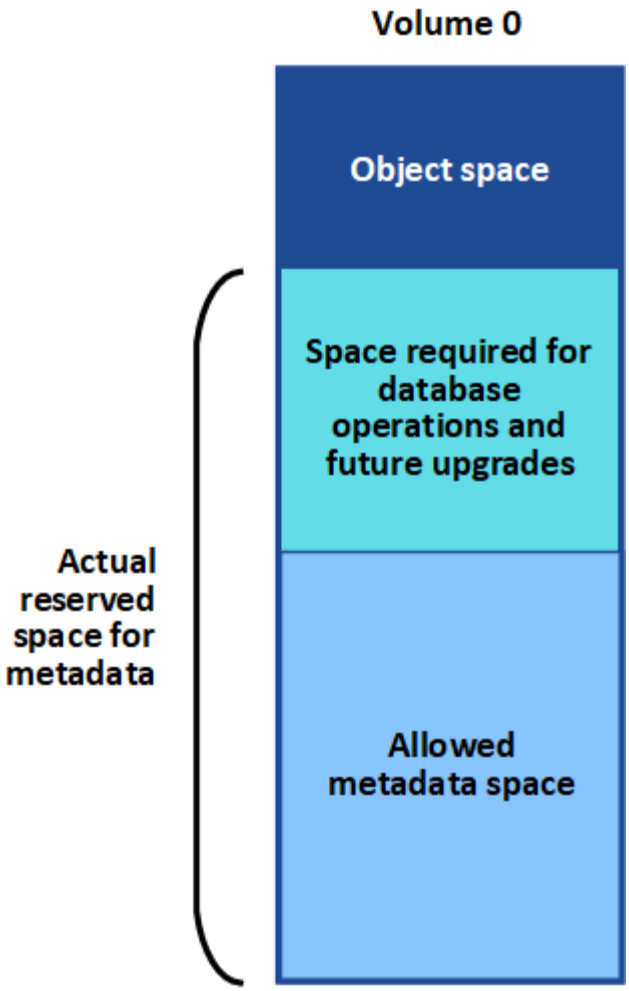
Se o alerta **armazenamento de metadados baixo** for acionado, você deverá adicionar novos nós de armazenamento.

Antes de começar

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

Sobre esta tarefa

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



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

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

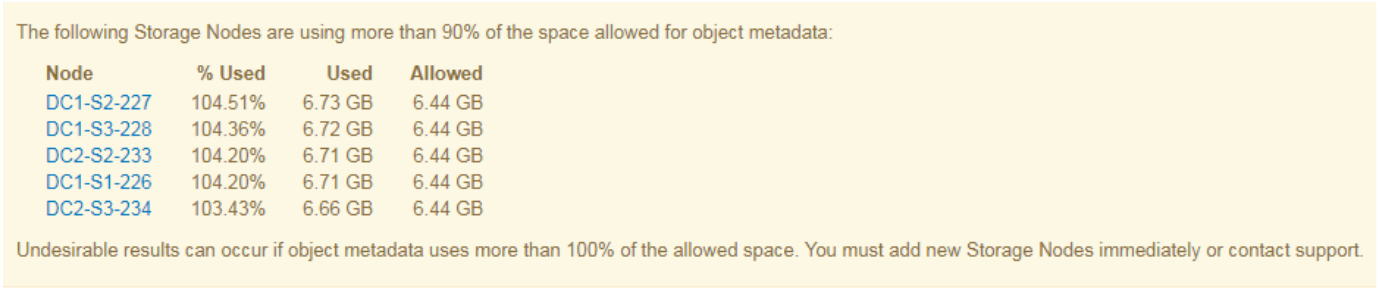
Quando essa expressão Prometheus atinge certos limites, o alerta **armazenamento de metadados baixo** é acionado.

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

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

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

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


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

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

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

Se o tamanho do volume 0 for menor do que a opção de armazenamento de espaço reservado de metadados (por exemplo, em um ambiente não-produção), o cálculo do alerta **armazenamento de metadados baixo** pode ser impreciso.

Passos

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

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

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

Serviços: Status - alarme Cassandra (SVST)

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

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

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

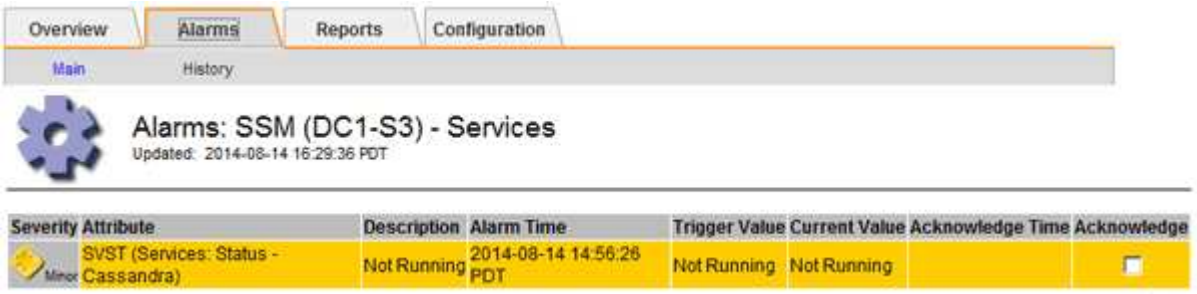
Você pode "execute o diagnóstico"obter informações adicionais sobre o estado atual da sua grade.

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

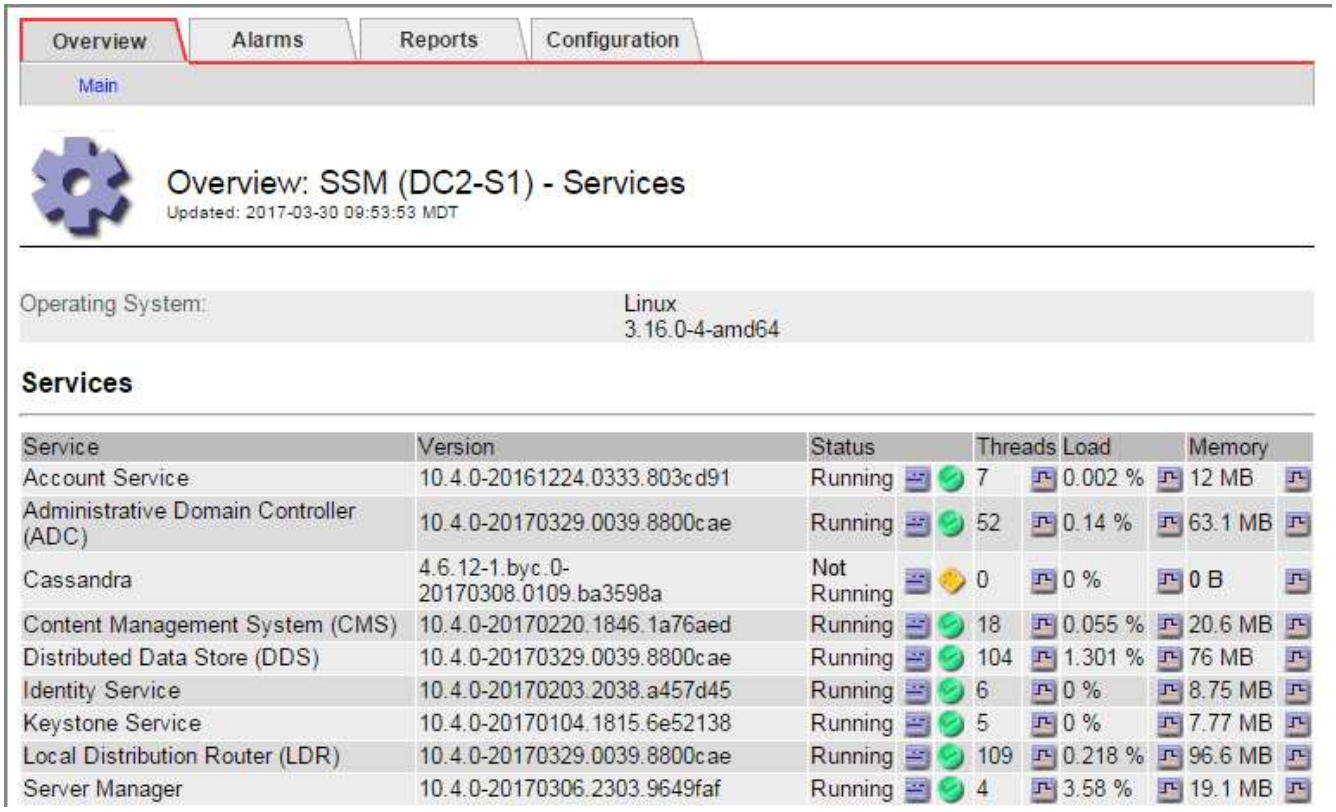
Passos

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

   Este exemplo mostra que o alarme SVST foi acionado.



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



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

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

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

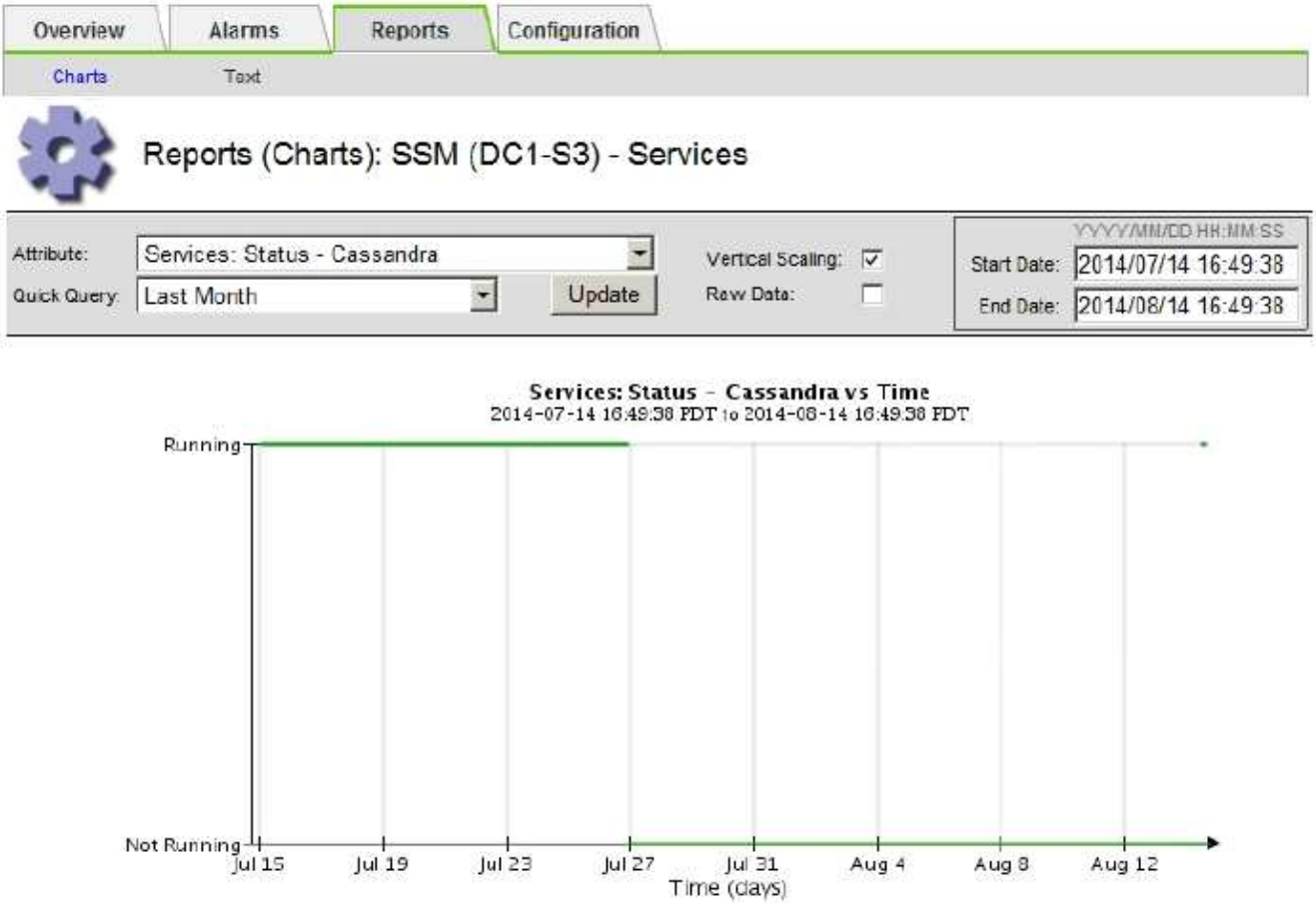
5. Para traçar o gráfico Cassandra:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**. Em seguida, selecione ***Site*** > ***Storage Node*** > **SSM** > **Serviços** > **relatórios** > **gráficos**.
   b. Selecione **Atributo** > **Serviço: Status - Cassandra**.
   c. Para **Data de Início**,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

fim, insira a data atual.

d. Clique em **Atualizar**.

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

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



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

   a. Faça login no nó da grade:

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

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

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

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

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

      O conteúdo do arquivo servermanager.log é exibido.

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

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

a. Certifique-se de que o carimbo de data/hora desta mensagem é o momento em que você tentou reiniciar o Cassandra conforme instruído na etapa Reinicie o Cassandra a partir do nó de storage.

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

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

   Para obter instruções, "Recupere o nó de storage abaixo mais de 15 dias"consulte .

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

Erros de memória sem Cassandra (alarme SMTT)

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

Sobre esta tarefa

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

Passos

1. Veja o evento:
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Expanda o site e selecione ***grid_node***.
   c. Selecione **SSM** e depois **Eventos** > **Configuração**.
2. Verifique se a contagem de erros de memória do Cassandra Heap é 1 ou superior.

   Você pode "execute o diagnóstico"obter informações adicionais sobre o estado atual da sua grade.

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

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

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

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

Solucionar erros de certificado

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

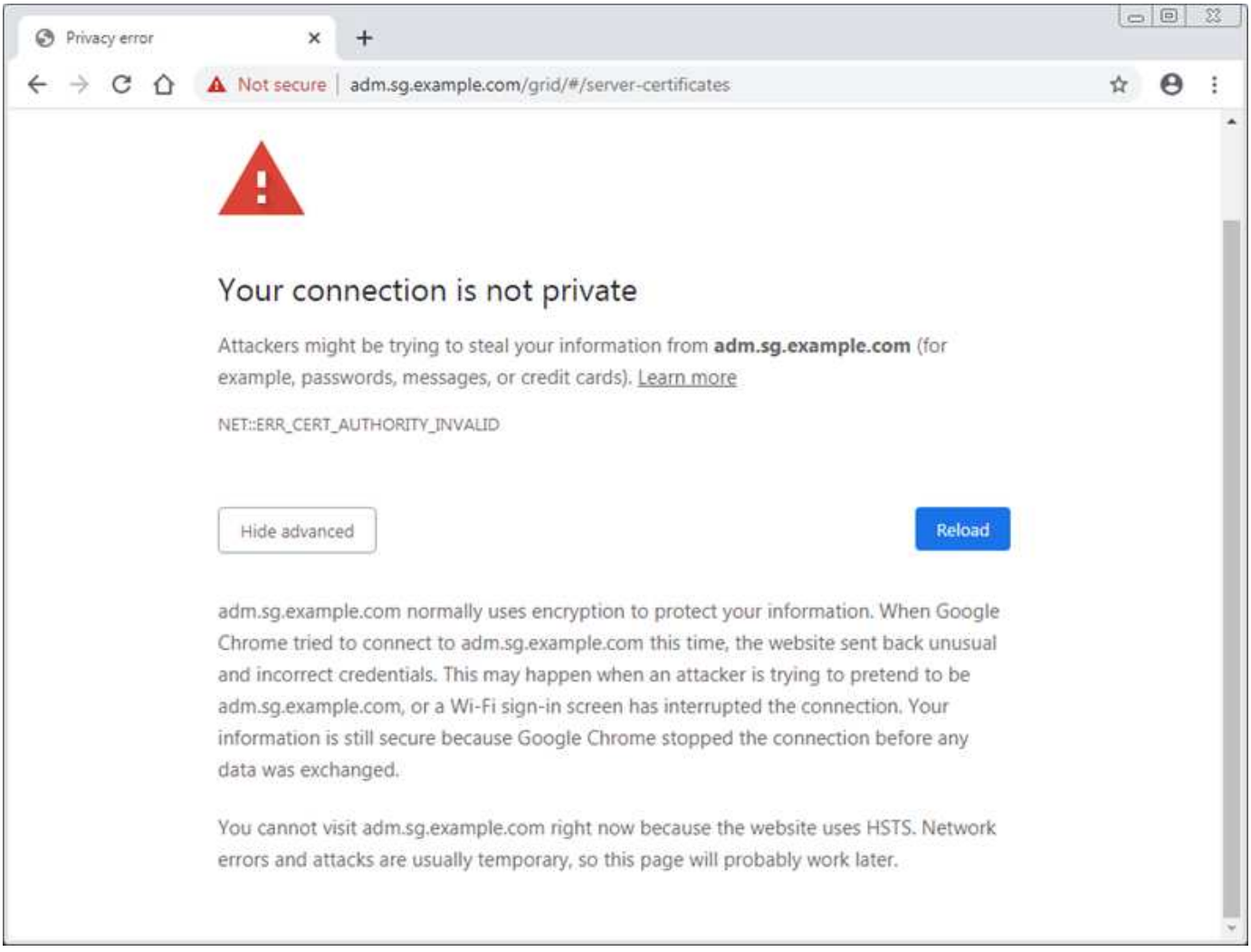
Sobre esta tarefa

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

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

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

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



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

Quando você estiver usando certificados de cliente para integração externa do Prometheus, erros de certificado podem ser causados pelo certificado de interface de gerenciamento do StorageGRID ou por certificados de cliente. O alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando um certificado de cliente está prestes a expirar.

Passos

Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado: . Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida"selecione a guia certificado apropriado", .

1. Verifique o período de validade do certificado. Alguns navegadores web e clientes S3 ou Swift não aceitam certificados com um período de validade superior a 398 dias.
2. Se o certificado tiver expirado ou expirar em breve, carregue ou gere um novo certificado.
   - Para obter um certificado de servidor, consulte as etapas "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"do .
   - Para obter um certificado de cliente, consulte as etapas "configurando um certificado de cliente"do .
3. Para erros de certificado de servidor, tente uma ou ambas as opções a seguir:
   - Certifique-se de que o nome alternativo do assunto (SAN) do certificado esteja preenchido e que a SAN corresponda ao endereço IP ou ao nome do host do nó ao qual você está se conetando.
   - Se você estiver tentando se conetar ao StorageGRID usando um nome de domínio:
     i. Insira o endereço IP do nó Admin em vez do nome de domínio para ignorar o erro de conexão e acessar o Gerenciador de Grade.
     ii. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida"selecione a guia certificado apropriado", instale um novo certificado personalizado ou continue com o certificado padrão.
     iii. Nas instruções de administração do StorageGRID, consulte as etapas "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"do .

Solucionar problemas de nó de administração e interface do usuário

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

Erros de início de sessão

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

Antes de começar

- Você tem o `Passwords.txt` arquivo.

- Você "permissões de acesso específicas"tem .

Sobre esta tarefa

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

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

Passos

1. Aguarde 10 minutos e tente iniciar sessão novamente.

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

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

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

   > ⓘ Se o SSO estiver ativado, você não poderá fazer logon usando uma porta restrita. Tem de utilizar a porta 443.

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

   Se a conta de usuário federada não estiver funcionando, tente fazer login no Gerenciador de Grade como um usuário local, como root.

   - Se o utilizador local puder iniciar sessão:
     i. Reveja todos os alarmes apresentados.
     ii. Selecione **CONFIGURATION** > **Access Control** > **Identity Federation**.
     iii. Clique em **Test Connection** para validar as configurações de conexão para o servidor LDAP.
     iv. Se o teste falhar, resolva quaisquer erros de configuração.
   - Se o usuário local não conseguir fazer login e tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.
6. Use o Secure Shell (ssh) para fazer login no Admin Node:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12. A partir do nó Admin, efetue login em cada um dos nós de armazenamento ADC, usando os endereços IP identificados.
    a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
    b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
    c. Digite o seguinte comando para mudar para root: `su -`
    d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

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

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

14. Repita as etapas Use Lumberjack para coletar logs e Rever registos para revisar os logs nos nós de storage.
15. Se você não conseguir resolver o problema, entre em Contato com o suporte técnico.

    Forneça os Registros que você coletou para o suporte técnico. Consulte também "Referência de ficheiros de registo".

Problemas na interface do usuário

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

Passos

1. Certifique-se de que está a utilizar um "navegador da web suportado".

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

2. Limpe o cache do navegador da Web.

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

Nó Admin indisponível

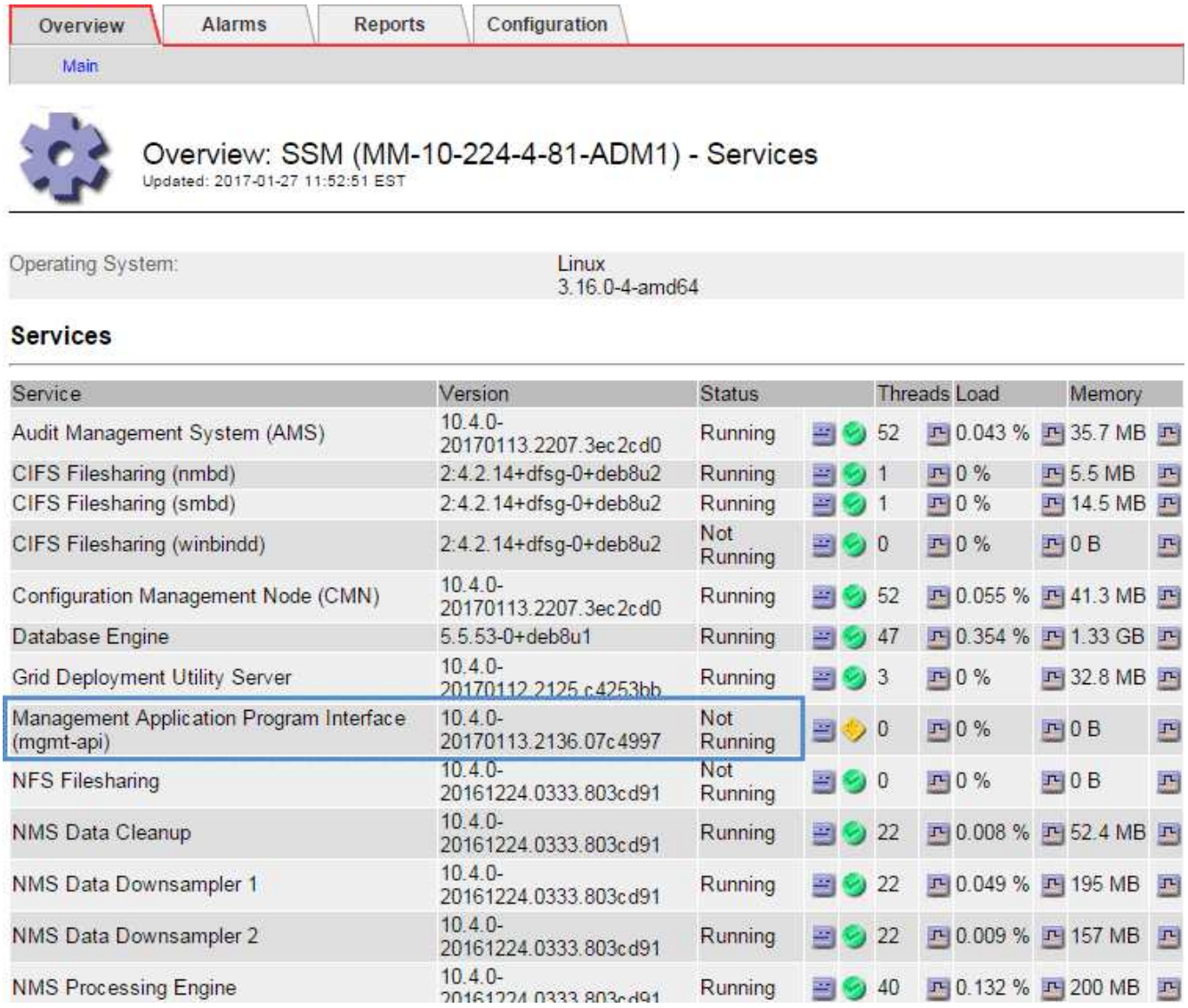
Se o sistema StorageGRID incluir vários nós de administração, você poderá usar outro nó de administração para verificar o status de um nó de administração indisponível.

Antes de começar

Você "permissões de acesso específicas"tem .

Passos

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



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

Solucionar problemas de rede, hardware e plataforma

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

"422: Entidade não processável" erros

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

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

Mensagem de erro	Causa raiz e ação corretiva

`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 ative Directory (AD).
	
	O uso da opção **não usar TLS** não é suportado para uso com servidores AD que imponham a assinatura LDAP. Você deve selecionar a opção **usar STARTTLS** ou a opção **usar LDAPS** para TLS.

`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)`
	Essa mensagem será exibida se você tentar usar uma cifra não suportada para fazer uma conexão TLS (Transport Layer Security) do StorageGRID para um sistema externo usado para identificar pools de federação ou armazenamento em nuvem.
	
	Verifique as cifras que são oferecidas pelo sistema externo. O sistema deve usar um dos "Cifras suportadas por StorageGRID" para conexões TLS de saída, como mostrado nas instruções de administração do StorageGRID.

Alerta de incompatibilidade da MTU da rede de Grade

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

Sobre esta tarefa

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

Passos

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

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

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

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

Argumentos posicionais	Descrição
`mtu`	A MTU a definir. Deve estar na faixa de 1280 a 9216.
`network`	As redes às quais aplicar a MTU. Inclua um ou mais dos seguintes tipos de rede: • grelha • 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.

Alarme de erro de receção de rede (NRER)

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

Sobre esta tarefa

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

StorageGRID:

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

Passos

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

Incompatibilidade de FEC

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

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

   Não é possível configurar as configurações do FEC nos dispositivos StorageGRID. Em vez disso, os aparelhos tentam descobrir e espelhar as configurações FEC nas portas do switch às quais estão conetados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC poderão não conseguir negociar uma configuração FEC comum. Sem uma configuração FEC comum, a rede voltará para o modo "no-FEC". Quando o FEC não está ativado, as conexões são mais suscetíveis a erros causados por ruído elétrico.

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

Incompatibilidade da MTU da porta do switch e da NIC

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

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

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

Consulte também "Altere a definição MTU" .

Altas taxas de erro de link

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

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

Buffer de anel NIC excedido

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

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

3. Depois de resolver o problema subjacente, redefina o contador de erros.
   a. Selecione **SUPPORT** > **Tools** > **Grid topology**.
   b. Selecione ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**.
   c. Selecione **Redefinir contagem de erros de recebimento** e clique em **aplicar alterações**.

Informações relacionadas

"Referência de alarmes (sistema legado)"

Erros de sincronização de tempo

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

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

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

Linux: Problemas de conetividade de rede

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

Clonagem de endereços MAC

Em alguns casos, os problemas de rede podem ser resolvidos usando a clonagem de endereços MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereços MAC para cada uma de suas redes como "verdadeiro" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contentor StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian".

> Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contentor StorageGRID pode fazer com que o sistema operacional do host se torne inacessível se o modo promíscuo não tiver sido ativado no hypervisor.

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

Modo promíscuo

Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para obter mais informações sobre como usar o modo promíscuo, consulte as instruções para "Red Hat Enterprise Linux" ou "Ubuntu ou Debian".

Linux: O status do nó é "órfão"

Um nó Linux em um estado órfão geralmente indica que o serviço StorageGRID ou o daemon de nó StorageGRID que controla o contentor do nó morreram inesperadamente.

Sobre esta tarefa

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

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

Passos

1. Verifique os logs do serviço daemon e do nó órfão para ver se há erros óbvios ou mensagens sobre sair inesperadamente.
2. Faça login no host como root ou usando uma conta com permissão sudo.
3. Tente iniciar o nó novamente executando o seguinte comando: `$ sudo storagegrid node start node-name`

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

Se o nó estiver órfão, a resposta será

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

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

   Para `seconds`, introduza o número de segundos que pretende aguardar que o recipiente pare (normalmente, 15 minutos ou menos). Por exemplo:

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

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

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

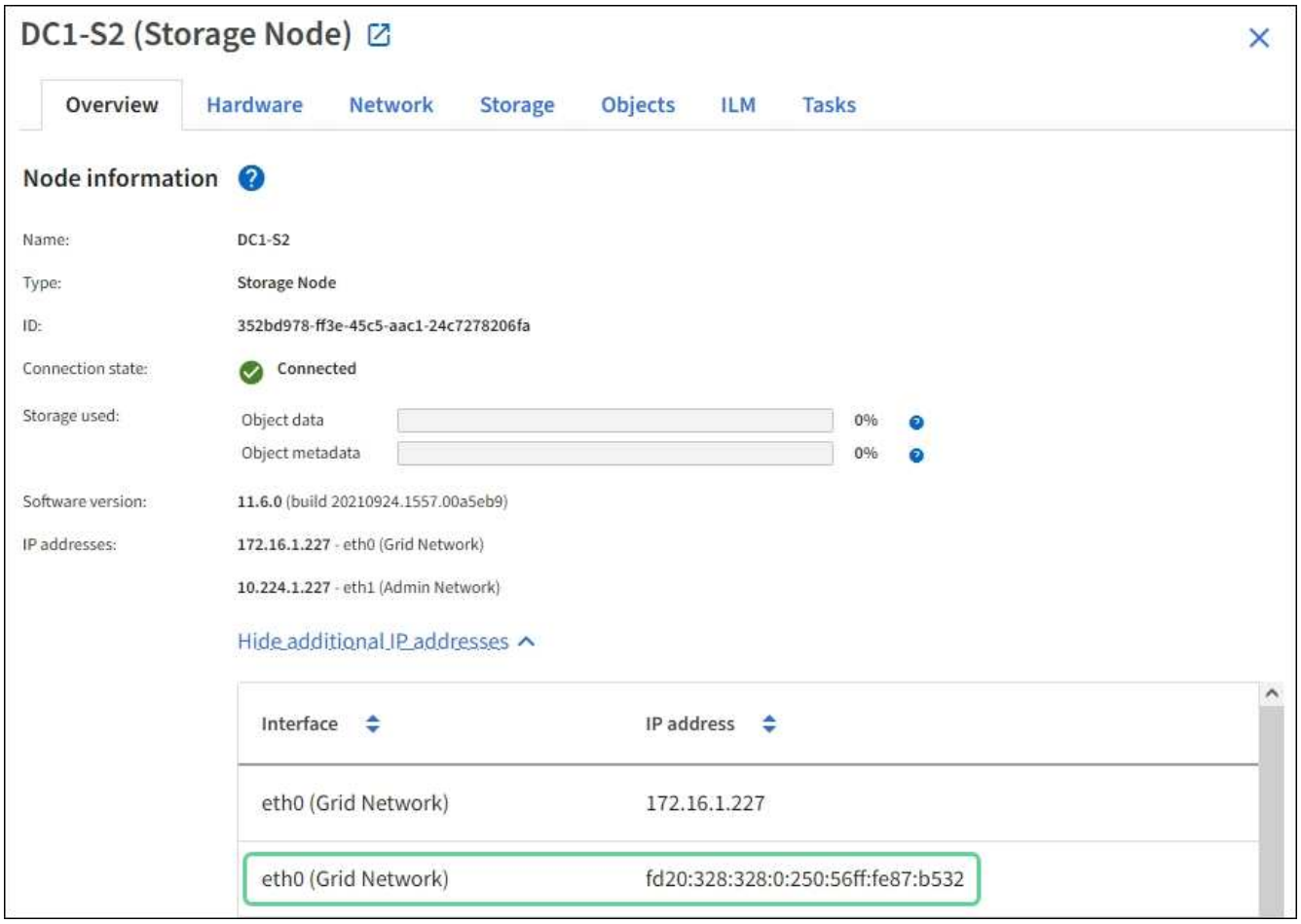
Linux: Solucione problemas de suporte ao IPv6

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

Sobre esta tarefa

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

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



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

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

Passos

1. Faça login no host como root ou usando 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 sistema operacional para alterar `sysctl` as configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Insira o contentor do nó StorageGRID: `storagegrid node enter node-name`

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

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

O resultado deve ser 1.

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

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

5. Saia do recipiente: `exit`

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

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

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

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

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

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

8. Execute estes comandos para reiniciar o contentor StorageGRID:

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

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

Solucionar problemas de um servidor syslog externo

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

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

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

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

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

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

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

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

Rever registos de auditoria

Revisar logs de auditoria: Visão geral

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e registos de auditoria do StorageGRID. Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções destinam-se aos administradores responsáveis pela produção de relatórios de atividade e

utilização do sistema que exijam a 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 Admin.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, "Configurar mensagens de auditoria e destinos de log"consulte .

Auditoria de fluxo e retenção de mensagens

Todos os serviços 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 `audit.log` o arquivo.

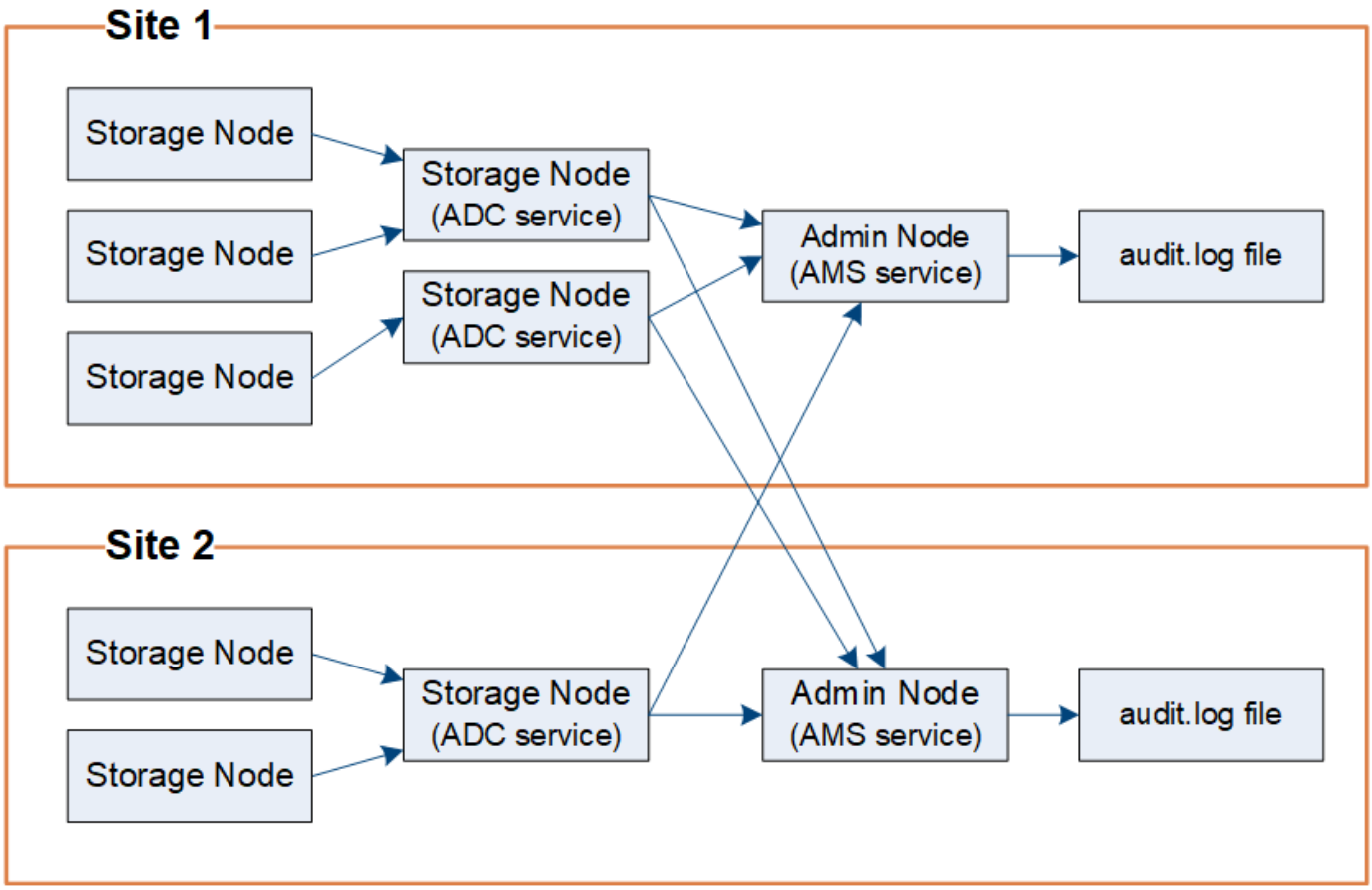
Auditoria do fluxo de mensagens

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 ADC no local do data center. O serviço ADC é ativado automaticamente para os três primeiros nós de storage instalados em cada local.

Por sua vez, cada serviço ADC atua como um relé e envia sua coleção de mensagens de auditoria para cada nó de administração no sistema StorageGRID, o que dá a cada nó de administração um Registro completo da atividade do sistema.

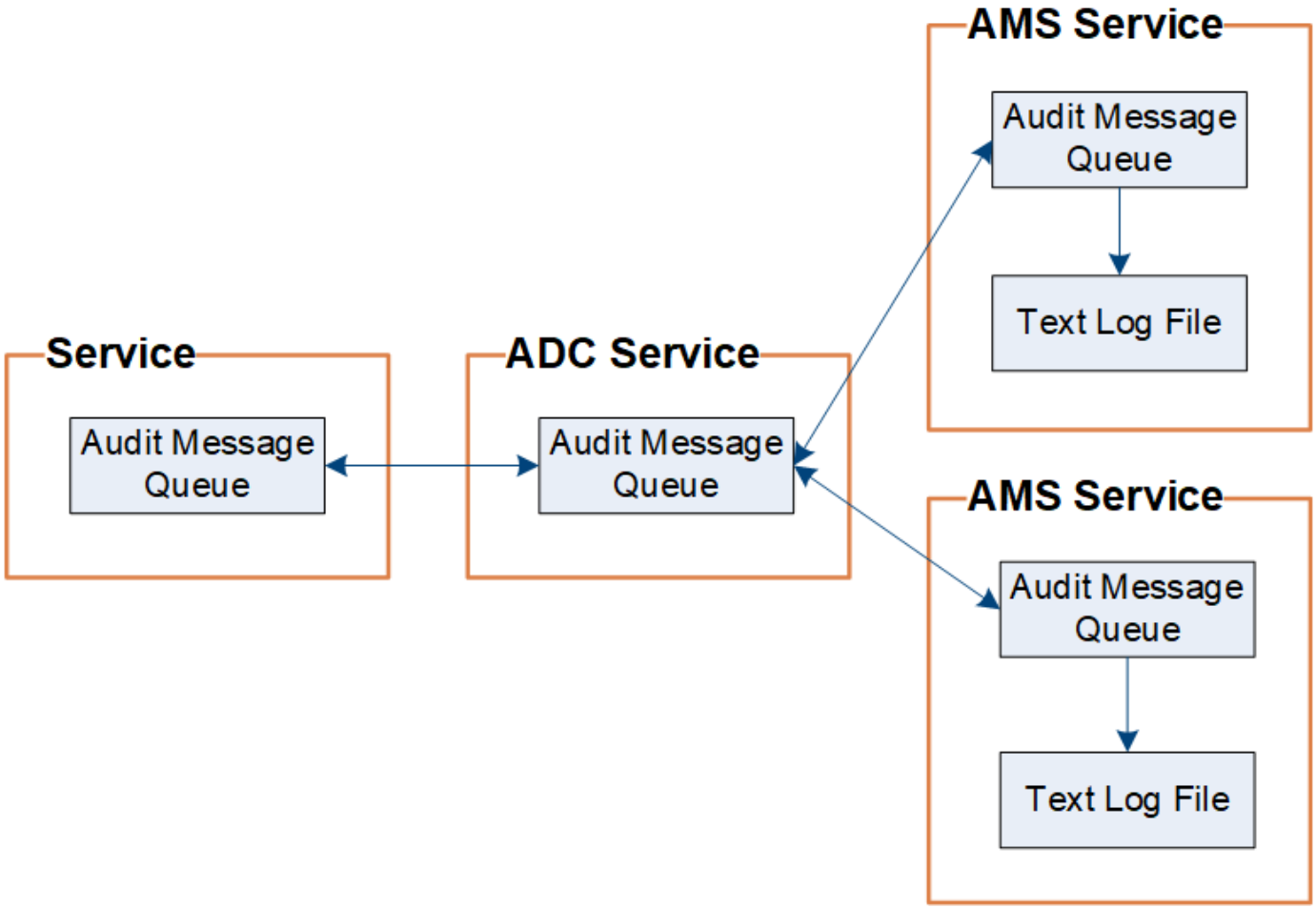
Cada nó Admin armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é `audit.log` nomeado .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de cópia e exclusão para garantir que nenhuma mensagem de auditoria seja perdida antes que ela possa 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 diretório do Admin Node `/var/local/log`. 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 conetividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível no diretório de cada nó `/var/local/`. 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` diretório usado por um nó Admin ficar cheio, o nó Admin será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações de clientes S3 e Swift não são afetadas. O alarme XAMS (Unreachable Audit Repositories) é acionado quando um repositório de auditoria é inacessível.
- Se o `/var/local/` diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para auditar mensagens até que o diretório esteja apenas 87% cheio. As solicitações de clientes S3 e Swift para outros nós não são afetadas. O alarme NRLY (relés de auditoria disponíveis) é acionado quando os relés de auditoria não são alcançáveis.

> ⓘ Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente `/var/local/log/localaudit.log` no arquivo.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 e Swift com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito grandes:

- A interrupção de um nó de administração ou de um nó de storage com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar com backlogged.
- Uma taxa de atividade contínua que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC se torna cheio por razões não relacionadas às mensagens de auditoria. Quando isso acontece, o nó pára 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 enfileiradas (AMQS)

Para ajudá-lo 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 administrador atinge determinados limites.

Se o alerta **fila de auditoria grande** 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 devem ser resolvidos com o tempo e podem ser ignorados.

Se o alerta ou o alarme persistir e aumentar a gravidade, veja 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 Desativado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora se ocorrer uma falha de rede ou nó. Por esse motivo, mensagens duplicadas podem existir no log de auditoria.

Acessar o arquivo de log de auditoria

O compartilhamento de auditoria contém o arquivo ativo `audit.log` e todos os arquivos de log de auditoria compatados. Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Passos

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

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

2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/log
```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos no diretório de um nó de administrador `/var/local/log`. Os arquivos de log de auditoria ativos são `audit.log` nomeados .

> 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 a ser gerados e armazenados quando um servidor syslog externo é configurado. "Configurar mensagens de auditoria e destinos de log"Consulte .

Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*. Se mais de um log de auditoria for criado em um único dia, os nomes de arquivo usarão a data em que o arquivo foi salvo, anexado por um número, no formato *`yyyy-mm-dd.txt.n`*. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são os primeiros e segundos 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 storage alocado para logs de auditoria no nó Admin. Um script monitora o consumo de espaço do log de auditoria e exclui 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 `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o 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: Visão geral

Os arquivos de log de auditoria são encontrados em cada nó Admin e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O tempo Universal coordenado (UTC) do evento que acionou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* estão 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 legibilidade). Essas mensagens foram geradas quando um locatário criou um bucket do 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]]
```

Em seu formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou

interpretar. Você pode usar o "ferramenta de auditoria-explicação" 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 demoraram.

Utilize a ferramenta de auditoria-explicação

Você pode usar a `audit-explain` ferramenta para traduzir as mensagens de auditoria no login de auditoria para um formato fácil de ler.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-explain` ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.

> ⓘ A `audit-explain` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-explain` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-explain` ferramenta. Essas quatro "SPUT"mensagens de auditoria foram geradas quando o locatário S3 com ID de conta 92484777680322627870 usou S3 SOLICITAÇÕES 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
```

A `audit-explain` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compatados. 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/*
  ```

- Aceite a entrada de um pipe, 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 partes que você deseja olhar e executar `audit-explain` nas partes, em vez de todo o arquivo.

> A `audit-explain` ferramenta não aceita arquivos compatados como entrada pipeada. Para processar arquivos compatados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   A `audit-explain` ferramenta imprime interpretações humanamente legíveis de todas as mensagens no arquivo ou arquivos especificados.

   > Para reduzir o comprimento das linhas e facilitar a legibilidade, os carimbos de data/hora não são apresentados por predefinição. Se você quiser ver os carimbos de data/hora, use a opção carimbo de data/hora (`-t`).

Use a ferramenta audit-sum

Você pode usar a `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-sum` ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

> A `audit-sum` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-sum` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
  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
```

A `audit-sum` ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria S3, Swift e ILM em um log de auditoria:

Código	Descrição	Consulte
ARCT	Recuperação de arquivamento do Cloud-Tier	"ARCT: Recuperação de arquivos do Cloud-Tier"
ASCT	Archive Store Cloud-Tier	"ASCT: Archive Store Cloud-Tier"
IDEL	ILM iniciado Excluir: Registra quando ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket.	"SDEL: S3 DELETE"

Código	Descrição	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: S3 CABEÇA"
SPUT	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 contentor.	"WDEL: Swift DELETE"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	"WGET: Rápido"
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	"WHEA: CABEÇA rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	"WPUT: Swift PUT"

A `audit-sum` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compatados. 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/*
```

- Aceite a entrada de um pipe, 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 compatados como entrada pipeada. Para processar arquivos compatados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Você pode usar as opções de linha de comando para resumir as operações em intervalos separadamente das operações em objetos ou agrupar resumos de mensagens por nome de intervalo, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo de operação mínimo, máximo e médio, mas você pode usar a `size (-s)` opção para olhar o tamanho do objeto.

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

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 a localização do arquivo ou arquivos que você deseja analisar:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
  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 de SGET (S3 GET) são as mais lentas em média em 1,13 segundos, mas as operações de SGET e SPUT (S3 PUT) mostram tempos piores longos de cerca de 1.770 segundos.

b. Para mostrar as operações de recuperação 10 mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicionar a opção de saída longa (`-l`) para incluir caminhos de objeto:

   ```
   grep SGET audit.log | audit-sum -l
   ```

   Os resultados incluem o tipo (objeto ou bucket) e o caminho, que permite que você grep o log de auditoria para 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 os três pedidos mais lentos de S3 GET foram para objetos de tamanho de cerca de 5 GB, que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos do pior caso.

3. Se você quiser determinar em que tamanhos de objetos estão sendo ingeridos e recuperados da grade, use a opção 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 do que o número de mensagens SGET, indicando que a maioria dos objetos nunca são recuperados.

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`), seguida 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 S3 RECEBEM tráfego aumentado entre 06:00 e 07:00. Os tempos máximos e médios são consideravelmente mais elevados nestes tempos também, e eles não aumentaram gradualmente à medida que a contagem aumentou. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

b. Para determinar que objetos de tamanho estavam sendo recuperados a cada hora ontem, adicione a opção 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 seu máximo.

c. Para ver mais detalhes, use o "ferramenta de auditoria-explicação" para rever todas as operações SGET durante essa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando grep for esperada para ser muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) de cada vez.

5. Se você quiser determinar se as operações do SPUT em buckets são mais lentas do que as operações do SPUT para objetos:

a. Comece usando a `-go` opção, que agrupa as 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 do SPUT para buckets têm caraterísticas de desempenho diferentes das operações do SPUT para objetos.

b. Para determinar quais buckets têm as operações de SPUT mais lentas, use a `-gb` opção, que agrupa as 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 as `-gb` opções e `-s`:

```
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 da mensagem de auditoria

Formato da mensagem de auditoria: Visão geral

As mensagens de auditoria trocadas no sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou a atividade que está sendo relatada.

Se as informações resumidas fornecidas pelas "auditoria-explicar"ferramentas e "soma de auditoria"forem insuficientes, consulte esta secção para compreender 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 cadeia de elementos de atributo. Toda a cadeia de carateres está entre colchetes (`[ ]`), e cada elemento de atributo na cadeia de carateres tem as seguintes caraterísticas:

- Entre os suportes `[ ]`
- Introduzido pela cadeia de carateres `AUDT`, que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de alimentação de linha `\n`

Cada elemento inclui um código de atributo, um tipo de dados 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 do atributo:

- `ATTR` é um código de quatro carateres para o atributo que está sendo relatado. Existem alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos para eventos.
- `type` É um identificador de quatro carateres 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 seguem sempre dois pontos (`:`). Os valores do tipo de dados CSTR são cercados por aspas duplas " ".

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo não assinado (32 bits); ele pode armazenar os números de 0 a 4.294.967.295.
UI64	Número inteiro duplo longo não assinado (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro carateres; um valor inteiro não assinado de 32 bits representado como quatro carateres ASCII, como "ABCD".
IPAD	Usado para endereços IP.
CSTR	Um array de comprimento variável de carateres UTF-8. Os carateres podem ser escapados com as seguintes convenções: • Barra invertida é. • O retorno do carro é r. • Aspas duplas. • A alimentação de linha (nova linha) é n. • Os carateres podem ser substituídos por seus equivalentes hexadecimais (no formato HH, 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 para um evento do sistema.

Após o contentor de abertura `[AUDT:` que identifica a própria mensagem, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrito pela mensagem de auditoria. Esses atributos são destacados no exemplo a seguir:

2018 11454 S3AI SGKH4 6002562159561124649 9 UI64-12 10.224.0 6002562159561124649 E6DYZKLUMRSKJA S3BK-05T08:24 100 S3AK 6002562159561124649 S3KY [AUDT:*[RSLT(FC32):SUCS]* *[TIME STR(UI64):45,921845 E4DA UI64 30720 UI32 10 UI64 1543998285921845 FC32 UI32 12281045 FC32 S3RQ UI64 15552417629170647261

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o "SHEA"código de mensagem ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
NO MEIO	FC32	ID do módulo: Um identificador de quatro carateres 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: O 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. Esta ID não pode ser alterada.
ASES	UI64	Identificador de sessão de auditoria: Em versões anteriores, este elemento indicou o momento em que o sistema de auditoria foi inicializado após o início do serviço. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: Em versões anteriores, esse contador foi incrementado para cada mensagem de auditoria gerada no nó de grade (ANID) e redefinido para zero na reinicialização do serviço. **Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: Um identificador que é compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.

Código	Tipo	Descrição
ATIM	UI64	Timestamp: A hora em que o evento foi gerado, que acionou a mensagem de auditoria, medida em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora para data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o carimbo de data/hora registado. 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 cadeia de carateres literal indicando o início do segmento de tempo da data. *`UUUUUU`* são microssegundos.
ATYP	FC32	Tipo de evento: Um identificador de quatro carateres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: Os atributos que estão incluídos.
AVER	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 retroativa no serviço AMS para processar mensagens de versões mais antigas de serviços.
RSLT	FC32	Resultado: O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será 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 gravado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é gravado 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. "SPUT" Representa uma transação S3 PUT, que Registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o intervalo 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 carimbo de data/hora Universal coordenada (UTC) no início da mensagem de auditoria. Este valor é uma versão legível por humanos 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]]
```

ATIM Registra o tempo, em microssegundos, desde o início da época UNIX. No exemplo, o valor `1405631878959669` é traduzido para Quinta-feira, 17-Jul-2014 21:17:59 UTC.

Auditar mensagens e o ciclo de vida do objeto

Quando são geradas mensagens de auditoria?

As 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 (S3 ou Swift).

As mensagens de auditoria são vinculadas por meio de identificadores específicos a cada protocolo.

Protocolo	Código
Ligar S3 operações	S3BK (balde), S3KY (chave) ou ambos
Ligando as operações Swift	WCON (container), WOBJ (objeto), ou ambos
Vinculação de operações internas	CBID (identificador interno do objeto)

Calendário das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós de grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar da mostrada nos exemplos nesta seção.

Nós de arquivamento

A série de mensagens de auditoria geradas quando um nó de arquivo envia dados de objeto para um sistema de armazenamento de arquivo externo é semelhante à dos nós de armazenamento, exceto que não há mensagem SCMT (Store Object Commit), e as mensagens ATCE (Archive Object Store Begin) e ASCE (Archive Object Store End) são geradas para cada cópia arquivada de dados de objeto.

A série de mensagens de auditoria geradas quando um nó de arquivo recupera dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que as mensagens ARCB (recuperação de objetos de arquivamento iniciada) e ARCE (fim de recuperação de objetos de arquivamento) são geradas para cada cópia recuperada de dados de objetos.

A série de mensagens de auditoria geradas quando um nó de arquivo exclui dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que não há nenhuma mensagem SREM (Object Store Remove) e há uma mensagem AREM (Archive Object Remove) para cada solicitação de exclusão.

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API (S3 ou Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de ingestão são incluídas.

S3 ingira mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SPUT	S3 COLOQUE a transação	Uma transação de ingestão de S3 PUT foi concluída com sucesso.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	"ORLM: Regras Objeto cumpridas"

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Traçado	Consulte
WPUT	Transação de COLOCAÇÃO rápida	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBID, WCON, WOBJ	"WPUT: Swift PUT"
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	"ORLM: Regras Objeto cumpridas"

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 fazer 2 cópias ILM.

> Nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de ingestão S3 (SPUT) estão listados.

Este exemplo assume que um bucket do 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 intervalo 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 Objeto cumpridas

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 aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume das localizações 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 apagamento, o campo LOCS inclui o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento

```
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 contentor 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]]
```

Eliminar transações

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas nas tabelas a

seguir. Apenas as mensagens necessárias para rastrear a transação de exclusão são incluídas.

S3 exclua mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SDEL	S3 Eliminar	Solicitação feita para excluir o objeto de um intervalo.	CBID, S3KY	"SDEL: S3 DELETE"

Swift delete mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
WDEL	Eliminação rápida	Solicitação feita para excluir o objeto de um recipiente ou do recipiente.	CBID, WOBJ	"WDEL: Swift DELETE"

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 são listadas no exemplo abaixo. Apenas os relacionados com a transação de exclusão S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objeto começa quando o cliente envia uma solicitação DeleteObject a um serviço LDR. A mensagem contém o intervalo do qual excluir o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
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]]
```

Recuperar transações objeto

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de recuperação são incluídas.

S3 mensagens de auditoria de recuperação

Código	Nome	Descrição	Traçado	Consulte
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Traçado	Consulte
WGET	Swift GET	Solicitação feita para recuperar um objeto de um contentor.	CBID, WCON, WOBJ	"WGET: Rápido"

Exemplo: Recuperação de objeto S3D.

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 são listadas no exemplo abaixo. Apenas os relacionados à transação de recuperação S3 (SGET) estão listados.

SGET: S3 GET

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject a um serviço LDR. A mensagem contém o intervalo do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
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 de bucket permitir, um cliente pode recuperar objetos anonimamente ou recuperar objetos de um bucket que é de propriedade de uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta de 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 ele não possui. Os valores para SBAI e SBAC Registram o ID e o nome da conta do locatário do proprietário do bucket, que difere do ID da conta do locatário e do nome do cliente registrado em S3AI e 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 Selecione em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, as mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são 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 Select S3 (o campo S3SR está 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

As mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados do S3

Código	Nome	Descrição	Traçado	Consulte
SUPD	S3 metadados atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBID, S3KY, HTRH	"SUPD: S3 metadados 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, cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO** > **Monitoramento** > **Auditoria e servidor syslog**). "Configurar mensagens de auditoria e destinos de log"Consulte .

```
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]]
```

Auditar mensagens

Mensagens de auditoria: Visão geral

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema são listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiramente 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 auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas alfabeticamente por seus códigos de quatro carateres. Esta lista alfabética permite-lhe encontrar informações sobre mensagens específicas.

Os códigos de quatro carateres utilizados ao longo deste capítulo são os valores ATYP encontrados nas mensagens de auditoria, como 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"

Auditar categorias de mensagens

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 nó de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Consulte
ECMC	Fragmento de dados com codificação de apagamento em falta: Indica que um fragmento de dados com codificação de apagamento em falta foi detetado.	"ECMC: Fragmento de dados codificado de apagamento em falta"
ECOC	Fragmento de dados codificado por apagamento corrompido: Indica que um fragmento de dados codificado por apagamento corrompido foi detetado.	"ECOC: Fragmento de dados codificado por apagamento corrompido"
ETAF	Falha na autenticação de segurança: Uma tentativa de conexão usando TLS (Transport Layer Security) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualizado ou registrado informações sobre si mesmo no sistema StorageGRID.	"GNRG: Registro GNDS"
GNUR	GNDS Unregistration: Um serviço não se registrou a partir do sistema StorageGRID.	"GNUR: GNDS Unregistration"
GTED	Tarefa de grelha terminada: O serviço CMN terminou de processar a tarefa de grelha.	"GTED: Tarefa de grelha terminada"
GTST	Tarefa de grade iniciada: O serviço CMN começou a processar a tarefa de grade.	"GTST: Tarefa de grade iniciada"
GTSU	Tarefa de grelha enviada: Uma tarefa de grelha foi enviada para o serviço CMN.	"GTSU: Tarefa de grelha enviada"
LLST	Localização perdida: Esta mensagem de auditoria é gerada quando um local é perdido.	"LLST: Localização perdida"
OLST	Objeto perdido: Um objeto solicitado não pode ser localizado dentro do sistema StorageGRID.	"OLST: O sistema detetou Objeto perdido"

Código	Título e descrição da mensagem	Consulte
ADICIONAR	Desativação da auditoria de segurança: O registo de mensagens de auditoria foi desativado.	"ADICIONAR: Desativação da auditoria de segurança"
SADE	Ativação da auditoria de segurança: O registo de mensagens de auditoria foi restaurado.	"SADE: Ativação da auditoria de segurança"
SVRF	Falha na verificação do armazenamento de objetos: Um bloco de conteúdo falhou verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
SVRU	Verificação desconhecido: Dados de objeto inesperados detetados no armazenamento de objetos.	"SVRU: Verificação do armazenamento de objetos desconhecido"
SYSD	Paragem nó: Foi solicitado um encerramento.	"SYSD: Parada do nó"
SIST	Parada do nó: Um serviço iniciou uma parada graciosa.	"SIST: Paragem 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 de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.

Código	Descrição	Consulte
APCT	Limpeza de arquivamento da camada da nuvem: Os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	"APCT: Purga de arquivamento do nível de nuvem"
ARCB	Início da recuperação de objetos de arquivamento: O serviço ARC inicia a recuperação de dados de objetos do sistema de armazenamento de arquivos externo.	"ARCB: Início da recuperação de objetos de arquivamento"

Código	Descrição	Consulte
ARCE	Fim de recuperação de objetos de arquivamento: Os dados de objetos foram recuperados de um sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de recuperação.	"ARCE: Fim de recuperação de objetos de arquivamento"
ARCT	Recuperação de arquivos do Cloud-Tier: Os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.	"ARCT: Recuperação de arquivos do Cloud-Tier"
ACEM	Remoção de objeto de arquivamento: Um bloco de conteúdo foi excluído com sucesso ou sem sucesso do sistema de armazenamento de arquivos externo.	"AFEM: Remoção de objetos de Arquivo"
ASCE	Fim do armazenamento de objetos de arquivamento: Um bloco de conteúdo foi gravado no sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de gravação.	"ASCE: Fim do armazenamento de objetos de Arquivo"
ASCT	Camada de nuvem: Os dados de objetos são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	"ASCT: Archive Store Cloud-Tier"
ATCE	Início do armazenamento de objetos de arquivamento: A gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.	"ATCE: Início do armazenamento de objetos de arquivo"
AVCC	Archive Validate Cloud-Tier Configuration: As configurações de conta e bucket fornecidas foram validadas com êxito ou sem sucesso.	"AVCC: Arquivamento Validar Configuração de nível de nuvem"
BROR	Pedido apenas de leitura do balde: Um balde entrou ou saiu do modo só de leitura.	"BROR: Pedido apenas de leitura do balde"
CBSE	Fim de envio de objeto: A entidade de origem concluiu uma operação de transferência de dados de nó de grade para nó de grade.	"CBSE: Fim de envio de objeto"
CBRE	Fim de recebimento de objeto: A entidade de destino concluiu uma operação de transferência de dados de nó de grade para nó de grade.	"CBRE: Fim de recebimento do objeto"

Código	Descrição	Consulte
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 de Grade cruzada"
EBDL	Esvaziar balde Excluir: O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazia).	"EBDL: Apagar balde vazio"
EBKR	Solicitação de balde vazio: Um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou parar de excluir objetos).	"EBKR: Pedido de balde vazio"
SCMT	Object Store commit: Um bloco de conteúdo foi completamente armazenado e verificado, e agora pode ser solicitado.	"SCMT: Solicitação de confirmação do armazenamento de objetos"
SREM	Remoção do armazenamento de objetos: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Armazenamento de objetos Remover"

O cliente lê mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Consulte
S3SL	S3 Selecionar solicitação: 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.	Cliente S3	"S3SL: S3 Selecione o pedido"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: S3 CABEÇA"

Código	Descrição	Usado por	Consulte
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	Cliente Swift	"WGET: Rápido"
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	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 ou Swift faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Consulte
OVWR	Object Overwrite: Registra uma transação para sobrescrever um objeto com outro objeto.	Clientes S3 e Swift	"OVWR: Substituição de objetos"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 DELETE"
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: S3 POST"
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket. **Nota:** se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	S3 metadados atualizados: Registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	"SUPD: S3 metadados atualizados"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	Cliente Swift	"WDEL: Swift DELETE"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	Cliente Swift	"WPUT: Swift PUT"

Mensagem de auditoria de gerenciamento

A categoria Gerenciamento Registra as solicitações do usuário para a API de

gerenciamento.

Código	Título e descrição da mensagem	Consulte
MGAU	Mensagem de auditoria da API de gerenciamento: Um log de solicitações de usuário.	"MGAU: Mensagem de auditoria de gestão"

Mensagens de auditoria 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	Consulte
IDEL	Exclusão iniciada ILM: Esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"
LKCU	Limpeza Objeto sobrescrita. 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 Objeto atendidas: Esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras ILM.	"ORLM: Regras Objeto cumpridas"

Referência da mensagem de auditoria

APCT: Purga de arquivamento do nível de nuvem

Essa mensagem é gerada quando os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi excluído.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. Sempre retorna 0.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.

Código	Campo	Descrição
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem do qual o objeto foi excluído.

ARCB: Início da recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma solicitação é feita para recuperar dados de objetos arquivados e o processo de recuperação é iniciado. Os pedidos de recuperação são processados imediatamente, mas podem ser reordenados para melhorar a eficiência da recuperação de meios lineares, como fita.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.
RSLT	Resultado	Indica o resultado do início do processo de recuperação do arquivo. O valor atualmente definido é:SUCS: A solicitação de conteúdo foi recebida e enfileirada para recuperação.

Esta mensagem de auditoria marca a hora de uma recuperação de arquivo. Ele permite que você combine a mensagem com uma mensagem final ARCE correspondente para determinar a duração da recuperação do arquivo e se a operação foi bem-sucedida.

ARCE: Fim de recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma tentativa do nó de arquivo para recuperar dados de objetos de um sistema de armazenamento de arquivos externo é concluída. Se for bem-sucedida, a mensagem indica que os dados do objeto solicitado foram completamente lidos a partir do local do arquivo e foram verificados com sucesso. Depois que os dados do objeto forem recuperados e verificados, eles serão entregues ao serviço solicitante.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.
VLID	Identificador de volume	O identificador do volume no qual os dados foram arquivados. Se uma localização de arquivo para o conteúdo não for encontrada, uma ID de volume de 0 será retornada.

Código	Campo	Descrição
RSLT	Resultado de recuperação	O estado de conclusão do processo de recuperação do arquivo: • SUCS: Bem-sucedido • VRFL: Falhou (falha na verificação de objetos) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • CANC: Falha (operação de recuperação cancelada) • GERR: Falhou (erro geral)

A correspondência desta mensagem com a mensagem ARCB correspondente pode indicar o tempo necessário para executar a recuperação do arquivo. Esta mensagem indica se a recuperação foi bem-sucedida e, em caso de falha, a causa da falha na recuperação do bloco de conteúdo.

ARCT: Recuperação de arquivos do Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se coneta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. O valor só é preciso para recuperações bem-sucedidas.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador único (UUID) do sistema de armazenamento de arquivos externo.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

AFEM: Remoção de objetos de Arquivo

A mensagem de auditoria Remover Objeto de Arquivo indica que um bloco de conteúdo foi excluído com sucesso ou sem sucesso de um nó de Arquivo. Se o resultado for bem-sucedido, o nó de arquivo informou com sucesso o sistema de armazenamento de arquivamento externo de que o StorageGRID liberou um local de objeto. Se o objeto é removido do sistema de armazenamento de arquivos externo depende do tipo de sistema e sua configuração.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de Mídia de arquivamento externo.
VLID	Identificador de volume	O identificador do volume no qual os dados do objeto foram arquivados.
RSLT	Resultado	O estado de conclusão do processo de remoção do arquivo: • SUCS: Bem-sucedido • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

ASCE: Fim do armazenamento de objetos de Arquivo

Esta mensagem indica que a gravação de um bloco de conteúdo em um sistema de armazenamento de arquivos externo terminou.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador do bloco de conteúdo armazenado no sistema de armazenamento de arquivos externo.
VLID	Identificador de volume	O identificador exclusivo do volume de arquivo no qual os dados do objeto são gravados.
VREN	Verificação ativada	Indica se a verificação é realizada para blocos de conteúdo. Os valores atualmente definidos são: • VENA: A verificação está ativada • VDSA: A verificação está desativada
MCLS	Classe de Gestão	Uma cadeia de carateres que identifica a classe de gerenciamento TSM à qual o bloco de conteúdo é atribuído, se aplicável.
RSLT	Resultado	Indica o resultado do processo de arquivo. Os valores atualmente definidos são: • SUCS: Bem-sucedido (processo de arquivamento bem-sucedido) • OFFL: Falhou (o arquivamento está offline) • VRFL: Falhou (verificação de objeto falhou) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

Esta mensagem de auditoria significa que o bloco de conteúdo especificado foi gravado no sistema de armazenamento de arquivos externo. Se a gravação falhar, o resultado fornece informações básicas de solução de problemas sobre onde a falha ocorreu. Informações mais detalhadas sobre falhas de arquivo podem ser encontradas examinando os atributos do nó de arquivo no sistema StorageGRID.

ASCT: Archive Store Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem para o qual o conteúdo foi armazenado.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

ATCE: Início do armazenamento de objetos de arquivo

Essa mensagem indica que a gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser arquivado.
VLID	Identificador de volume	O identificador exclusivo do volume para o qual o bloco de conteúdo é escrito. Se a operação falhar, um ID de volume de 0 é retornado.

Código	Campo	Descrição
RSLT	Resultado	Indica o resultado da transferência do bloco de conteúdo. Os valores atualmente definidos são: • SUCS: Sucesso (bloco de conteúdo armazenado com sucesso) • EXIS: Ignorado (bloco de conteúdo já estava armazenado) • ISFD: Falha (espaço em disco insuficiente) • STER: Falhou (erro ao armazenar o CBID) • OFFL: Falhou (o arquivamento está offline) • GERR: Falhou (erro geral)

AVCC: Arquivamento Validar Configuração de nível de nuvem

Essa mensagem é gerada quando as configurações são validadas para um tipo de destino Cloud Tiering - Simple Storage Service (S3).

Código	Campo	Descrição
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	UUID associado ao sistema de armazenamento de arquivamento externo sendo validado.

BROR: Pedido apenas de leitura do balde

O serviço LDR gera essa mensagem de auditoria quando um intervalo entra ou sai do modo somente leitura. Por exemplo, um intervalo entra no modo somente leitura enquanto todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do balde	A ID do balde.
BROV	Valor da solicitação somente leitura do balde	Se o intervalo está sendo feito somente leitura ou está deixando o estado somente leitura (1: Somente leitura, 0: Não-somente leitura).
JOGOS DE BROS	Motivo apenas de leitura do balde	A razão pela qual o intervalo está sendo feito somente leitura ou deixando o estado somente leitura. Por exemplo, emptyBucket.
S3AI	S3 ID da conta do locatário	O ID da conta de locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.

Código	Campo	Descrição
S3BK	Balde S3	O nome do bucket S3.

CBRB: Início de recebimento de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes 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, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do 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 iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas 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: Fim de recebimento do objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do 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 iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.

Código	Campo	Descrição
RSLT	Resultado da transferência	O resultado da operação de transferência (do ponto de vista da entidade de envio): SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: Conexão perdida durante a transferência CTMO: Tempo limite de conexão durante o estabelecimento ou transferência UNRE: ID do nó de destino inalcançável CRPT: A transferência terminou devido à receção de dados corrompidos ou inválidos

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objetos

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes 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, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do 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 iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.

Código	Campo	Descrição
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas 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 de envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do 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 iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.

Código	Campo	Descrição
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.
RSLT	Resultado da transferência	O resultado da operação de transferência (do ponto de vista da entidade de envio): SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: Conexão perdida durante a transferência CTMO: Tempo limite de conexão durante o estabelecimento ou transferência UNRE: ID do nó de destino inalcançável CRPT: A transferência terminou devido à receção de dados corrompidos ou inválidos

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CGRR: Solicitação de replicação de Grade cruzada

Essa 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 grade que abrangem uma atualização do StorageGRID 11,7 para 11,8 podem ter um tamanho total de objeto impreciso.
S3AI	S3 ID da conta do locatário	O ID da conta de locatário que possui o bucket do qual o objeto está sendo replicado.

Código	Campo	Descrição
GFID	ID de ligação da federação da grelha	O ID da conexão de federação de grade sendo usado para replicação entre grade.
OPER	Operação CGR	O tipo de operação de replicação entre redes que foi tentada: • 0: Replique objeto • 1: Replique objeto multipart • 2: Replique o marcador de exclusão
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo.
VSID	ID da versão	O ID da versão da versão específica de um objeto que estava sendo replicado.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou erro geral (GERR).

EBDL: Apagar balde vazio

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazia).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.
CAMINHO	S3 balde/chave	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
RSLT	Resultado da operação de eliminação	O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente.

EBKR: Pedido de balde vazio

Essa mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o

bucket vazio (ou seja, para excluir objetos do bucket ou parar de excluir objetos).

Código	Campo	Descrição
BUID	UUID do balde	A ID do balde.
EBJS	Configuração JSON do bucket vazio	Contém o JSON que representa a configuração atual de bucket vazio.
S3AI	S3 ID da conta do locatário	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

ECMC: Fragmento de dados codificado de apagamento em falta

Esta mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento em falta.

Código	Campo	Descrição
VCMC	ID VCS	O nome do VCS que contém o pedaço em falta.
MCID	Código bloco	O identificador do fragmento codificado de apagamento em falta.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificado por apagamento corrompido

Essa mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento corrompido.

Código	Campo	Descrição
VCCO	ID VCS	O nome do VCS que contém o bloco corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido codificado de apagamento.
CCID	Código bloco	O identificador do fragmento codificado de apagamento corrompido.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' 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 TLS (Transport Layer Security) falhou.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP sobre a qual a autenticação falhou.
RUIDA	Identidade do usuário	Um identificador dependente do serviço que representa a identidade do utilizador remoto.
RSLT	Código de motivo	O motivo da falha: SCNI: Falha no estabelecimento de conexão segura. CERM: O certificado estava ausente. CERT: Certificado 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 ausentes. UCRI: As credenciais do usuário eram inválidas. UCRU: As credenciais do usuário não foram permitidas. TOUT: A autenticação expirou.

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e a lógica adicional incorporada ao serviço. Se esta autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, é registada uma mensagem de auditoria. Isso permite consultas para tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota ter uma configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Essa mensagem de auditoria deve ser

monitorada para detetar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera essa mensagem de auditoria quando um serviço atualizou ou registrou 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 de nó	O ID do nó do serviço que iniciou a solicitação de atualização.
GNTP	Tipo de dispositivo	O tipo de dispositivo do nó de grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A cadeia de carateres que identifica a versão do modelo do dispositivo do nó de 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	O endereço IP do nó da grade.

Essa mensagem é gerada sempre que um nó de grade atualiza sua entrada no Grid Nodes Bundle.

GNUR: GNDS Unregistration

O serviço CMN gera essa mensagem de auditoria quando um serviço tem informações não registradas sobre si mesmo a partir do sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID de nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grelha terminada

Esta mensagem de auditoria indica que o serviço CMN terminou de processar a tarefa de grade especificada e moveu a tarefa para a tabela Histórico. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria Grid Task Started correspondente. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	Código 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, neste 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 de grade foi concluída com sucesso. • ABRT: A tarefa de grade foi encerrada sem um erro de reversão. • ROLF: A tarefa de grade foi encerrada e não foi possível concluir o processo de reversão. • CANC: A tarefa de 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 uma duplicata.

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 de tarefa de Grade enviada para tarefas de grade iniciadas pelo serviço de envio de tarefa de Grade interno e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela pendente, essa mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	Código 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, neste 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 grelha enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	Código tarefa	Identifica de forma única 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, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.
TTYP	Tipo tarefa	O tipo de tarefa de grade.
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição tarefa	Uma descrição humanamente legível da tarefa de grade.
CUBAS	Válido após Timestamp	A primeira vez (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do Timestamp	A última hora (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.

Código	Campo	Descrição
TSRC	Fonte	A origem da tarefa: • TXTB: A tarefa de grade foi enviada pelo sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada através do Serviço interno de envio de tarefa de Grade.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi submetida para ativação automática. • PEND: A tarefa de 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: ILM iniciou Excluir

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 ou contentores Swift**. 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
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CMPA	Conformidade: Eliminação automática	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o intervalo esteja sob uma retenção legal.
CMPL	Conformidade: Guarda legal	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se o balde está atualmente sob uma retenção legal.

Código	Campo	Descrição
CMPR	Conformidade: Período de retenção	Apenas para objetos em buckets compatíveis com S3. O comprimento do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Apenas para objetos em buckets compatíveis com S3. O 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 intervalo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em baldes não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCALIZAÇÃO	Locais	O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído). CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto. CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	• Se um objeto em um bucket compatível com S3 estiver sendo excluído automaticamente porque seu período de retenção expirou, esse campo estará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se aplicam atualmente ao objeto, este campo mostra o rótulo legível por humanos da última regra ILM aplicada ao objeto.

Código	Campo	Descrição
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão 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

Essa mensagem é gerada quando o StorageGRID remove um objeto sobrescrito que antes era necessário limpar para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 ou Swift 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 uso interno.*
LUID	UUUID Objeto removido	O identificador do objeto que foi removido.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto que ainda existe. Este valor só está disponível se o objeto não tiver sido excluído.

LLST: Localização perdida

Essa mensagem é gerada sempre que um local para uma cópia de objeto (replicado ou codificado por apagamento) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBID	O CBID afetado.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por apagamento. O ID do perfil de codificação de apagamento usado.
LTYP	Tipo de localização	CLDI (Online): Para dados de objeto replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
PCLD	Caminho para o objeto replicado	O caminho completo para a localização do disco dos dados do objeto perdido. Somente retornado quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Toma 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. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de acionamento	UTILIZADOR: Utilizador acionado SIST: Sistema acionado
UUID	ID universal única	O identificador do objeto afetado no sistema StorageGRID.

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento Registra as solicitações do usuário para a API de gerenciamento. Cada solicitação que não é uma solicitação GET ou HEAD para a API Registra uma resposta com o nome de usuário, IP e tipo de solicitação para a API.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome de domínio do host.

Código	Campo	Descrição
MPAT	PATH da solicitação	O caminho da solicitação.
MPQP	Parâmetros de consulta de solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo do pedido	O conteúdo do corpo do pedido. Enquanto o corpo da resposta é 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 de resposta, elas são retiradas do corpo de solicitação para os seguintes métodos POST: • Nome de usuário e ID de conta em **POST autorize** • Nova configuração de sub-redes em **POST /grid/grid-networks/update** • Novos servidores NTP em **POST /Grid/ntp-server/update** • IDs de servidor desativadas em **POST /Grid/Servers/Deactivation** **Nota:** as 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: • POST • COLOQUE • ELIMINAR • PATCH
MRSC	Código de resposta	O código de resposta.
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. **Nota:** as informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN de utilizador	A URNA (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.

OLST: O sistema detetou Objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar cópias de um objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto perdido.
NOID	ID de nó	Se disponível, a última localização direta ou próxima do objeto perdido conhecida. É possível ter apenas o ID do nó sem um ID de volume se as informações do volume não estiverem disponíveis.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	Se disponível, o nome do bucket S3 e o nome da chave S3 ou o nome do contentor Swift e o identificador do objeto Swift.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.
UUID	ID universal única	O identificador do objeto perdido dentro do sistema StorageGRID.
VOLI	ID do volume	Se disponível, o ID de volume do nó de armazenamento ou nó de arquivo para a última localização conhecida do objeto perdido.

ORLM: Regras Objeto cumpridas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras ILM.

> A mensagem ORLM não é gerada quando um objeto é armazenado com êxito pela regra de fazer cópias 2 padrão se outra regra na política usar o filtro avançado tamanho do objeto.

Código	Campo	Descrição
BUID	Colhedor do balde	Campo ID do balde. Usado para operações internas. Aparece apenas se STAT for PRGD.
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCALIZAÇÃO	Locais	O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído). CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto. CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível por humanos dado à regra ILM aplicada a este objeto.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
SGCB	CBID do recipiente	CBID do recipiente para o objeto segmentado. Este valor está disponível apenas para objetos segmentados e multipartes.
STAT	Estado	O estado da operação ILM. Feito: Operações ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação 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 universal único	O identificador do objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
VSID	ID da versão	A 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 ocorrer um dos seguintes eventos:

- As regras de ILM para o objeto são satisfeitas para sempre.
- As regras de ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano deteta que uma cópia dos dados de objetos replicados está corrompida. O sistema StorageGRID executa uma avaliação ILM para substituir o objeto corrompido.

Informações relacionadas

- "Transações de ingestão de objetos"
- "Eliminar transações"

OVWR: Substituição de objetos

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo (novo)	O CBID para o novo objeto.
CSIZ	Tamanho Objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.
OCBD	Identificador de bloco de conteúdo (anterior)	O CBID para o objeto anterior.
UUID	ID universal única (novo)	O identificador do novo objeto dentro do sistema StorageGRID.
OUID	ID universal única (anterior)	O identificador para o objeto anterior dentro do sistema StorageGRID.
CAMINHO	S3 ou Swift Object Path	O caminho de objeto S3 ou Swift usado para o objeto anterior e novo

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação de Sobreposição de objetos. O resultado é sempre: SUCS: Bem-sucedido
SGRP	Local (Grupo)	Se presente, o objeto sobrescrito foi excluído no local especificado, que não é o local onde o objeto sobrescrito foi ingerido.

S3SL: S3 Selecione o pedido

Esta mensagem regista uma conclusão depois de uma solicitação de seleção S3 ter sido devolvida 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 digitalizados	Número de bytes verificados (recebidos) dos nós de storage. BYSC e BYPR provavelmente serão diferentes se o objeto estiver compactado. Se o objeto for compactado, o BYSC teria a contagem de bytes compatados e o BYPR seria os bytes após a descompressão.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "bytes digitalizados" foram realmente processados ou agidos por uma tarefa S3 Select.
BYRT	Bytes retornados	Número de bytes que um trabalho S3 Select retornou ao cliente.
REPR	Registos processados	Número de Registros ou linhas que uma tarefa S3 Select recebeu de nós de storage.
RERT	Registos devolvidos	Número de Registros ou linhas que um trabalho S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se o S3 Select job finished processing or not (Selecionar trabalho concluído ou não). Se isso for falso, a tarefa não foi concluída e os campos de erro provavelmente terão dados neles. 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, levou para que o S3 Select Job fosse concluído.
ERMG	Mensagem de erro	Mensagem de erro gerada pela tarefa S3 Select.

Código	Campo	Descrição
ERTY	Tipo de erro	Tipo de erro que o S3 Select job gerou.
ERST	Erro Stacktrace	Erro Stacktrace gerado pela tarefa S3 Select.
S3BK	Balde S3	O nome do bucket S3.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O ID da chave de acesso S3 para o usuário que enviou a solicitação.
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo.

ADICIONAR: Desativação da auditoria de segurança

Essa 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	Ativar método	O método utilizado para desativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para desativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente ativado, mas agora foi desativado. Normalmente, isso é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SADE: Ativação da auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registo de mensagens de auditoria; as mensagens de auditoria estão novamente a ser recolhidas e entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para ativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para ativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente desativado (SADD), mas foi agora restaurado. Isso geralmente é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SCMT: Confirmação de armazenamento de objetos

O conteúdo da grade não é disponibilizado ou reconhecido como armazenado até que ele tenha sido comprometido (ou seja, ele foi armazenado persistentemente). O conteúdo armazenado persistentemente foi completamente gravado no disco e passou por verificações de integridade relacionadas. Essa mensagem é emitida quando um bloco de conteúdo é comprometido com o armazenamento.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com o armazenamento permanente.
RSLT	Código do 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 DELETE

Quando um cliente S3 emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou bucket especificado ou para remover um subrecurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.

Código	Campo	Descrição
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em baldes não incluem este campo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em baldes não incluem este campo.
GFID	ID ligação Federação grelha	O ID de conexão da conexão de federação de grade associada a uma solicitação de exclusão de replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
GFSA	Código conta origem Federação grelha	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `` `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for 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	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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 único universal para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens de log de auditoria especificam UUDM ou UUUUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto, e UUID indica um objeto.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 GET

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket ou remover um subrecurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LITY	ListObjectsV2	Foi solicitada uma resposta *v2 format*. Para obter detalhes, "AWS ListObjectsV2" consulte . Apenas para operações DO balde GET.
NCHD	Número de crianças	Inclui chaves e prefixos comuns. Apenas para operações DO balde GET.
RANG	Leitura de intervalo	Apenas para operações de leitura de gama. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho de todo o objeto.
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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.
TRNC	Truncado ou não truncado	Defina como false se todos os resultados foram retornados. Defina como verdadeiro se mais resultados estiverem disponíveis para retornar. Apenas para operações DO balde GET.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: S3 CABEÇA

Quando um cliente S3 emite uma TRANSAÇÃO PRINCIPAL, 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
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. As operações em baldes não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `` `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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 universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: S3 POST

Quando um cliente S3 emite uma solicitação POST Object, essa mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo 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 cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). (Não esperado para SPOS).
RSLT	Código do resultado	Resultado da solicitação de RestoreObject. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Código	Campo	Descrição
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável. Defina como "Select" (selecionar) para uma operação de seleção S3D.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	Restaurar informações.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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 universal único	O identificador do objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
VSID	ID da versão	O ID da versão 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 subrecurso bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes não incluem este campo.
CMPS	Definições de conformidade	As configurações de conformidade usadas ao criar o bucket, se estiverem presentes na solicitação (truncadas para os primeiros 1024 carateres).
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.
GFID	ID ligação Federação grelha	O ID de conexão da conexão de federação de grade associada a uma solicitação PUT DE replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.
GFSA	Código conta origem Federação grelha	O ID da conta do locatário na grade de origem para uma solicitação DE COLOCAÇÃO DE replicação entre grade. Incluído apenas nos registos de auditoria na grelha de destino.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for 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 Objeto ativado	Valor do cabeçalho da solicitação `x-amz-bucket-object-lock-enabled` , se presente na solicitação.
LKLH	Bloqueio Objeto retenção legal	Valor do cabeçalho da solicitação `x-amz-object-lock-legal-hold` , se estiver presente na solicitação PutObject.
LKMD	Modo de retenção de bloqueio de objetos	Valor do cabeçalho da solicitação `x-amz-object-lock-mode` , se estiver presente na solicitação PutObject.
LKRU	Reter Data até bloqueio Objeto	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date` , se estiver presente na solicitação PutObject.
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	A nova configuração de subrecursos (truncada para os primeiros 1024 carateres).
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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.
UID	ID de carregamento	Incluído apenas nas mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as peças foram carregadas e montadas.

Código	Campo	Descrição
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	A 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 controle de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "Habilitado" ou "suspenso". As operações em objetos não incluem este campo.

SREM: Armazenamento de objetos Remover

Essa mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não é mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código do resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Essa 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: S3 metadados atualizados

Essa 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
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em baldes 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.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em baldes não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para pedidos anónimos.
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 universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão 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 os dados de objeto 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 ingeridos no sistema. Se alguma dessas verificações falhar, o sistema coloca automaticamente em quarentena os dados de objeto replicados corrompidos para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou a verificação.

Código	Campo	Descrição
RSLT	Código do resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação HMAC (hash-based message Authentication code). 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 ruim.

Esta mensagem deve ser monitorada de perto. Falhas de verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar que operação acionou a mensagem, consulte o valor do campo AID (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 do armazenamento de objetos 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 detetada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do ficheiro	O caminho do arquivo da cópia de objeto inesperada.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' 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 objetos foram detetadas 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 parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, esta mensagem é enviada apenas após um reinício subsequente, porque a fila de mensagens de auditoria não é eliminada antes do encerramento. Procure a mensagem DO SISTEMA, enviada no início da sequência de encerramento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

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".

SIST: Paragem do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. O SYST pode ser usado para determinar se o desligamento foi solicitado, antes que o serviço seja reiniciado (ao contrário do SYSD, que normalmente é enviado após o reinício do serviço).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem DO SISTEMA não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, essa mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa. 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 a descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (uma vez que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Server Manager reinicia automaticamente um serviço com falha.

WDEL: Swift DELETE

Quando um cliente Swift emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou contentor especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local 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 universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores 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: Rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contentor ou listar os contentores em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e containers não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e containers não incluem esse campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do 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 universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e containers não incluem esse 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 PRINCIPAL, uma solicitação é feita para verificar a existência de uma conta, contentor ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e containers não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e containers não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO PRINCIPAL. 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 universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e containers não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: Swift PUT

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contentor. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. `X-Forwarded-For` É incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do 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 universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.

Código	Campo	Descrição
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores 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