Monitorar e solucionar problemas

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/pt-br/storagegrid-120/monitor/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

Índice

Monitore e solucione problemas em um sistema StorageGRID . . . 1
Monitorar o sistema StorageGRID . . . 1
Monitore um sistema StorageGRID . . . 1
Visualize e gerencie o dashboard no StorageGRID . . . 1
Veja a página de nós . . . 4
Informações para monitorar regularmente . . . 37
Gerenciar alertas . . . 67
Referência de arquivos de log . . . 105
Configurar o gerenciamento de logs e o servidor syslog externo . . . 125
Use o monitoramento SNMP . . . 139
Coletar dados adicionais do StorageGRID . . . 151
Solucione problemas do sistema StorageGRID . . . 165
Solucione problemas em um sistema StorageGRID . . . 165
Solucionar problemas de objetos e storage . . . 172
Solucione problemas de metadados no StorageGRID . . . 191
Solucionar problemas de erros de certificado no StorageGRID . . . 193
Solucionar problemas do nó de administração e da interface de usuário no StorageGRID . . . 194
Solucione problemas de rede, hardware e plataforma no StorageGRID . . . 198
Solucionar problemas de mensagens de erro do servidor syslog externo para StorageGRID . . . 205
Saiba mais sobre problemas de armazenamento em cache do balanceador de carga no StorageGRID . . . 208
Analisar registros de auditoria . . . 209
Mensagens e logs de auditoria . . . 209
Como as mensagens de auditoria se movem pelo sistema StorageGRID até o arquivo de log de auditoria para retenção . . . 210
Acesse os arquivos de log de auditoria a partir da linha de comando do nó Admin do StorageGRID . . . 213
Saiba mais sobre a rotação de arquivos de log de auditoria no StorageGRID . . . 214
Formato do arquivo de log de auditoria . . . 214
Formato da mensagem de auditoria . . . 227
Mensagens de auditoria e o ciclo de vida do objeto . . . 232
Mensagens de auditoria . . . 238

Monitore e solucione problemas em um sistema StorageGRID

Monitorar o sistema StorageGRID

Monitore um sistema StorageGRID

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

Antes de começar

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

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

Sobre esta tarefa

Estas instruções descrevem como:

- "Visualize e gerencie o painel de controle"
- "Veja a página de nós"
- "Monitore regularmente estes aspectos do sistema:"
  - "Saúde do sistema"
  - "Capacidade de armazenamento"
  - "Gerenciamento de ciclo de vida"
  - "Recursos de rede e sistema"
  - "Atividade do tenant"
  - "Operações de balanceamento de carga"
  - "Conexões de federação de grid"
- "Gerenciar alertas"
- "Visualizar arquivos de log"
- "Configurar o gerenciamento de logs e o servidor syslog externo"
- "Use um servidor syslog externo"para coletar informações de auditoria
- "Utilize SNMP para monitoramento"
- "Alterar a priorização de E/S"alterar as prioridades relativas das operações de E/S

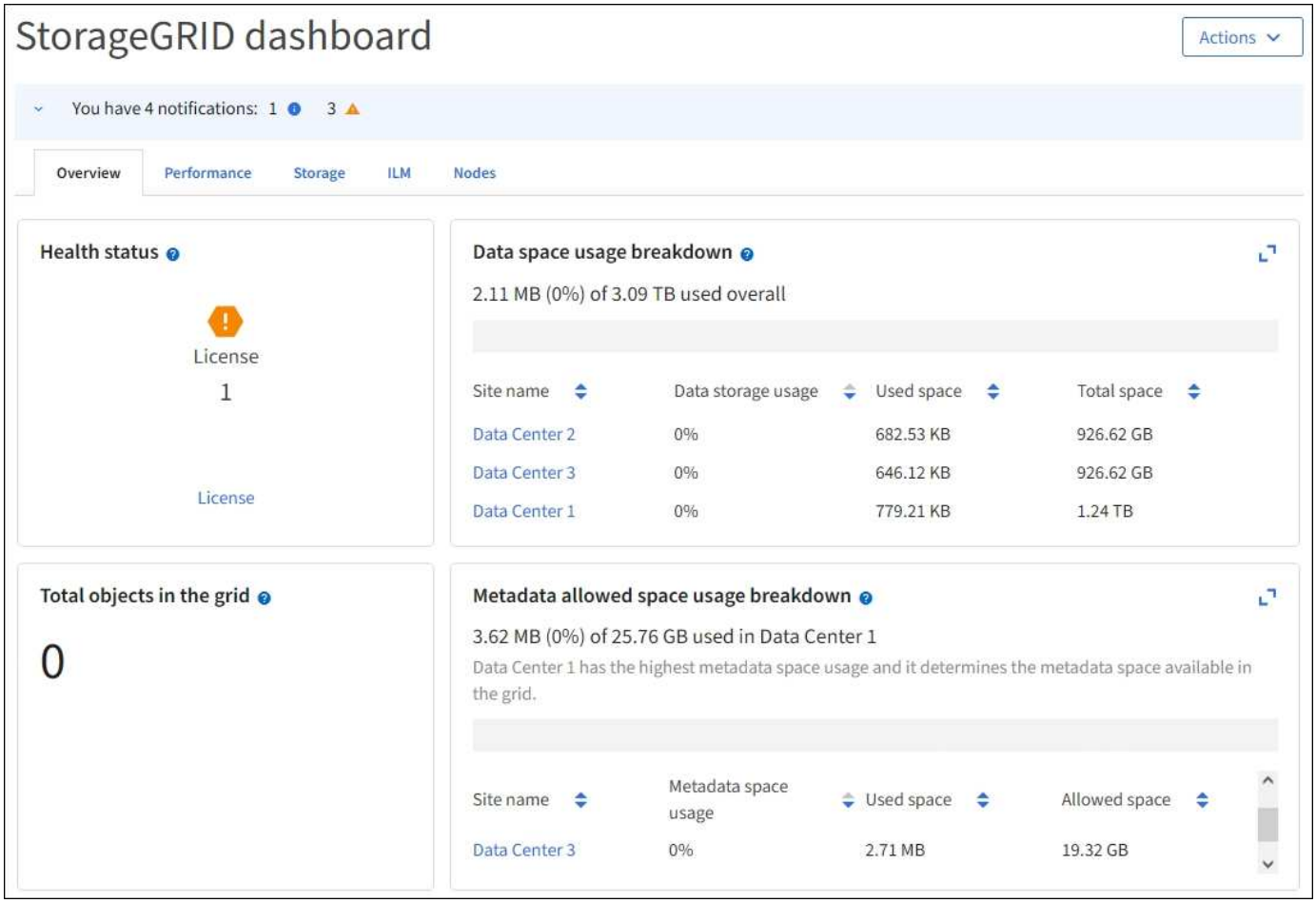
Visualize e gerencie o dashboard no StorageGRID

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

implementação do StorageGRID.

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

Seu painel de controle pode ser diferente dependendo da configuração do sistema.



Veja o dashboard

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

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

As abas do painel de controle fornecidas pelo sistema contêm cartões com os seguintes tipos de informação:

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

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

Algumas das cartas podem ser maximizadas para facilitar a visualização. Selecione o ícone de maximizar no canto superior direito da carta. Para fechar uma carta maximizada, selecione o ícone de minimizar ou selecione **Close**.

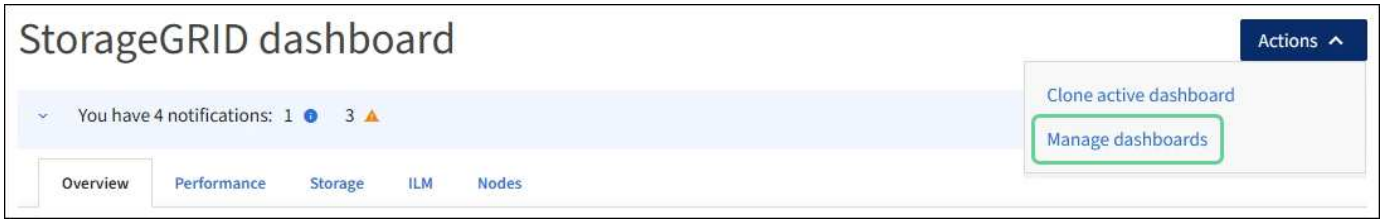
Gerenciar painéis de controle

Se você tiver acesso de root (consulte "Permissões do grupo de administradores"), você pode executar as seguintes tarefas de gerenciamento para painéis:

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

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

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



Configurar dashboards

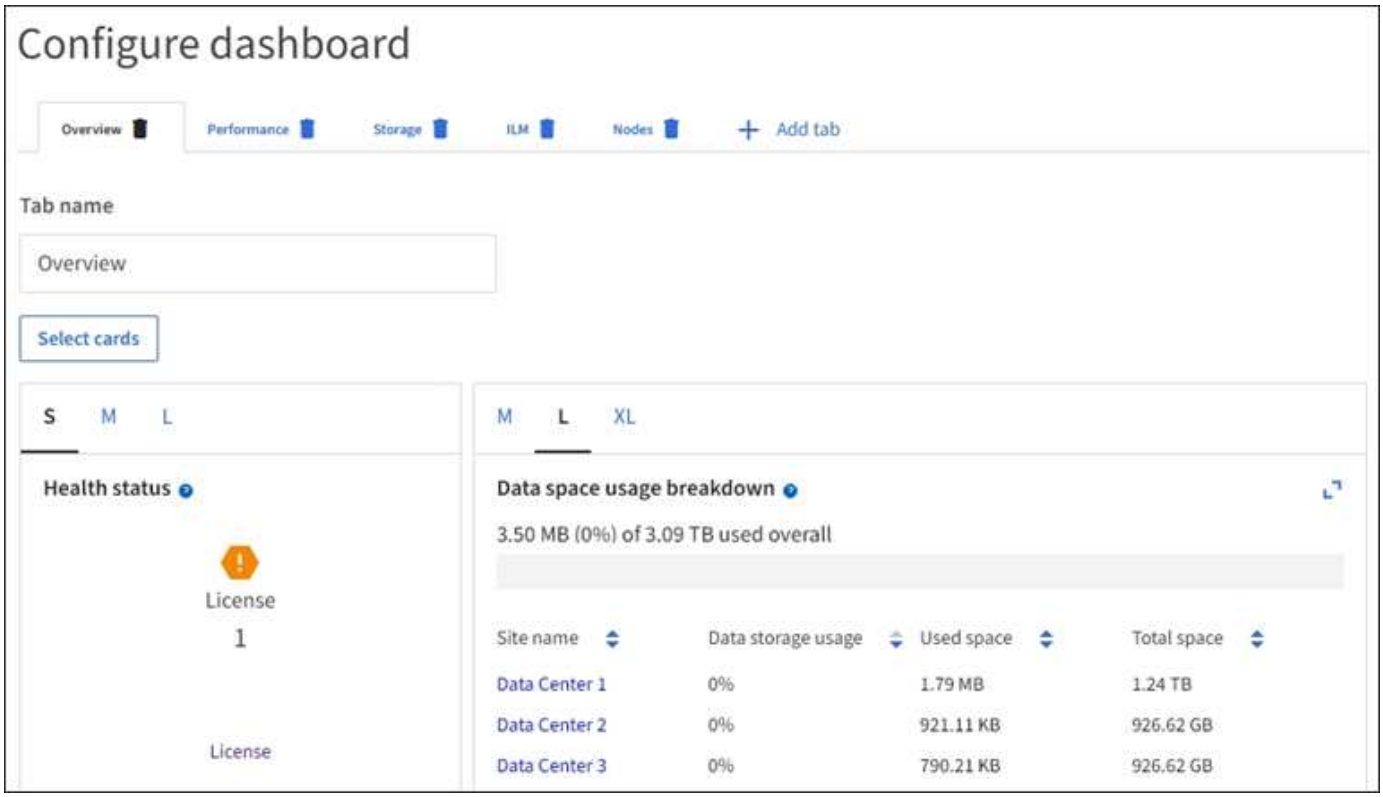
Para criar um novo painel clonando o painel ativo, selecione **Ações** > **Clonar painel ativo**.

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

O painel de controle fornecido pelo sistema não pode ser editado nem removido.

Ao configurar um dashboard, você pode:

- Adicionar ou remover abas
- Renomeie as abas e dê nomes únicos às novas abas
- Adicione, remova ou reorganize (arraste) os cartões para cada aba
- Selecione o tamanho para cada cartão escolhendo **S**, **M**, **L** ou **XL** na parte superior do cartão



Veja a página de nós

Veja a página de nós do StorageGRID

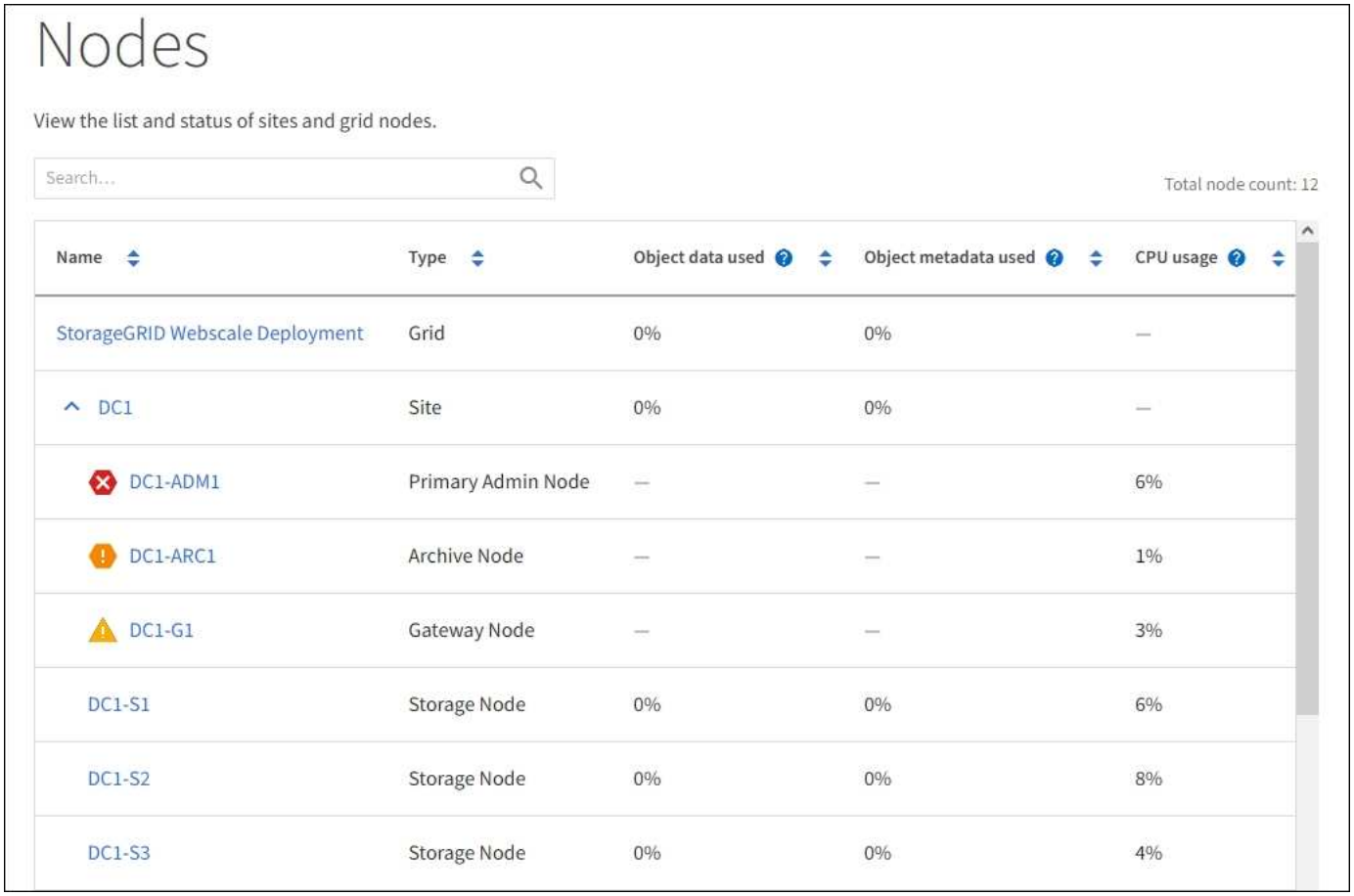
Quando você precisar de informações mais detalhadas sobre o seu sistema StorageGRID do que as fornecidas pelo painel, você pode usar a página Nós para visualizar métricas de toda a grade, de cada site na grade e de cada nó em um site.

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

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

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

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



Ícones de estado da conexão

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

Ícone	Descrição	Ação necessária
	Não conectado - Desconhecido Por razões desconhecidas, um nó é desconectado ou os serviços no nó são interrompidos inesperadamente. Por exemplo, um serviço no nó pode ter sido interrompido ou o nó pode ter perdido a conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta **Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. "Selecione cada alerta" e siga as ações recomendadas. Por exemplo, você pode precisar reiniciar um serviço que parou ou reiniciar o host do nó. **Nota**: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	Sem conexão - administrativamente inativo Por um motivo previsível, o nó não está conectado à grid. Por exemplo, o nó, ou os serviços no nó, foi desligado corretamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Dependendo do problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Verifique se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos, "Selecione cada alerta" siga as ações recomendadas.

Se um nó estiver desconectado do grid, ele pode ter um alerta subjacente, mas apenas o ícone "Não conectado" aparece. Para ver os alertas ativos de um nó, selecione o nó.

Ícones de alerta

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

Crítico: Existe uma condição anormal que interrompeu o funcionamento normal de um nó ou serviço do StorageGRID. Você deve resolver o problema imediatamente. A não resolução do problema pode resultar em interrupção do serviço e perda de dados.

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

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

Veja os detalhes de um sistema, site ou nó

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

Para visualizar as informações da grade, do site ou do nó:

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

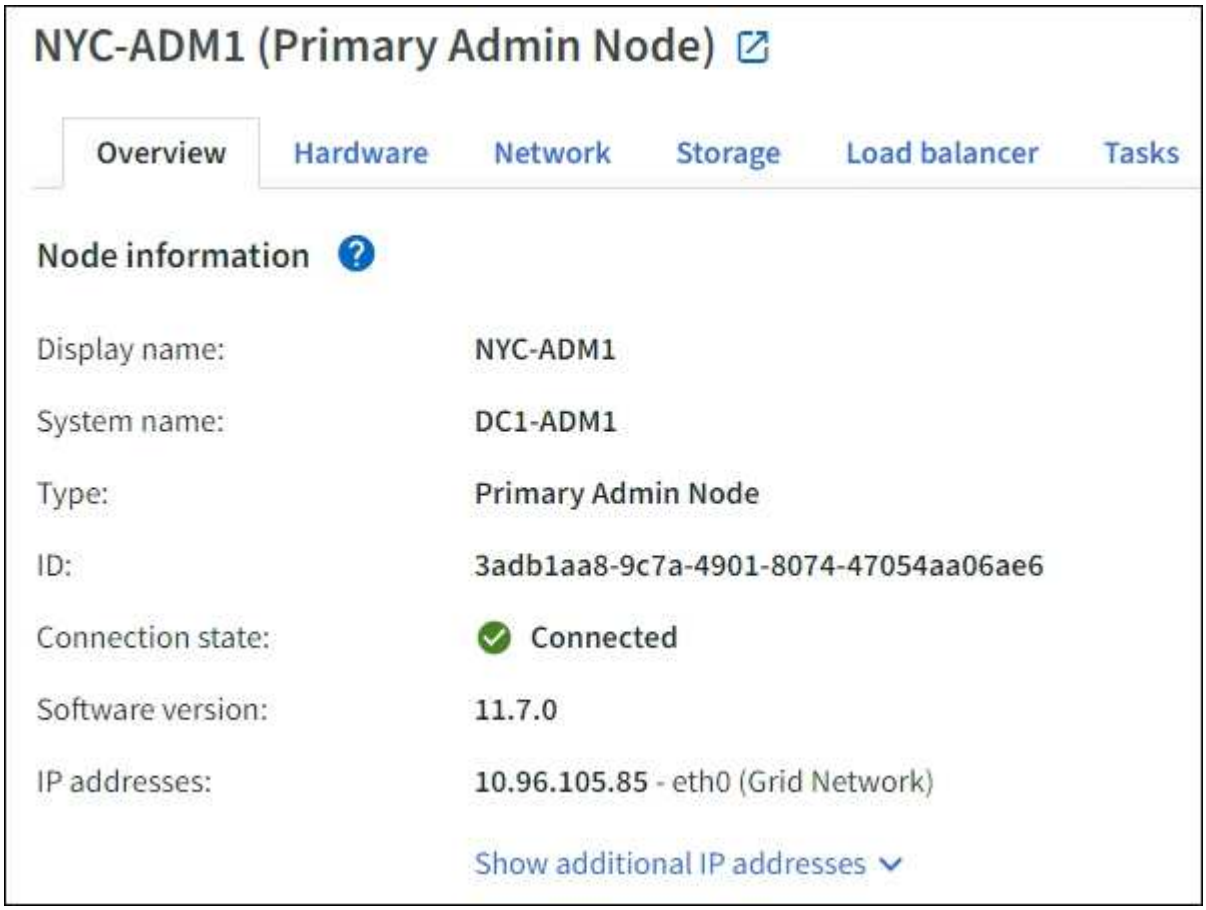
Veja a guia Visão geral do StorageGRID

A aba Visão geral fornece informações básicas sobre cada nó. Ela também mostra quaisquer alertas que estejam afetando o nó no momento.

A aba Visão geral é exibida para todos os nós.

Informações do nó

A seção Informações do Nó da aba Visão Geral lista informações básicas sobre o nó.



As informações gerais de um nó incluem o seguinte:

- **Nome de exibição** (mostrado somente se o nó tiver sido renomeado): o nome de exibição atual do nó. Use o procedimento "Renomeie a grade, os sites e os nós" para atualizar esse valor.
- **Nome do sistema**: O nome que você inseriu para o nó durante a instalação. Os nomes de sistema são usados para operações internas do StorageGRID e não podem ser alterados.
- **Tipo**: o tipo de nó — Admin Node, primary Admin Node, Storage Node ou Gateway Node.
- **ID**: O identificador único do nó, que também é chamado de UUID.
- **Estado da conexão**: Um de três estados. O ícone correspondente ao estado mais grave é exibido.
  - **Desconhecido**: Por algum motivo desconhecido, o nó não está conectado à rede ou um ou mais serviços estão inesperadamente indisponíveis. Por exemplo, a conexão de rede entre os nós foi perdida, a energia caiu ou um serviço está inativo. O alerta **Unable to communicate with node** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.

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

  - **Administrativamente inativo**: o nó não está conectado à grid por um motivo esperado. Por exemplo, o nó, ou os serviços no nó, foi desligado corretamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.
  - **Conectado**: o nó está conectado à rede.
- **Armazenamento utilizado**: Apenas para Storage Nodes.
  - **Dados do objeto**: A porcentagem do espaço total utilizável para dados do objeto que foi utilizada no Storage Node.
  - **Metadados de objeto**: A porcentagem do espaço total permitido para metadados de objeto que foi utilizada no Storage Node.
- **Versão do software**: A versão do StorageGRID instalada no nó.
- **Grupos HA**: Apenas para Admin Node e Gateway Nodes. Exibe se uma interface de rede no nó está incluída em um grupo de alta disponibilidade e se essa interface é a interface primária.
- **Endereços IP**: Os endereços IP do nó. Clique em **Mostrar endereços IP adicionais** para visualizar os endereços IPv4 e IPv6 do nó e os mapeamentos de interface.

Alertas

A seção Alertas da guia Visão geral lista todos os "alertas que estão afetando este nó e que ainda não foram silenciados" alertas. Selecione o nome do alerta para visualizar detalhes adicionais e ações recomendadas.

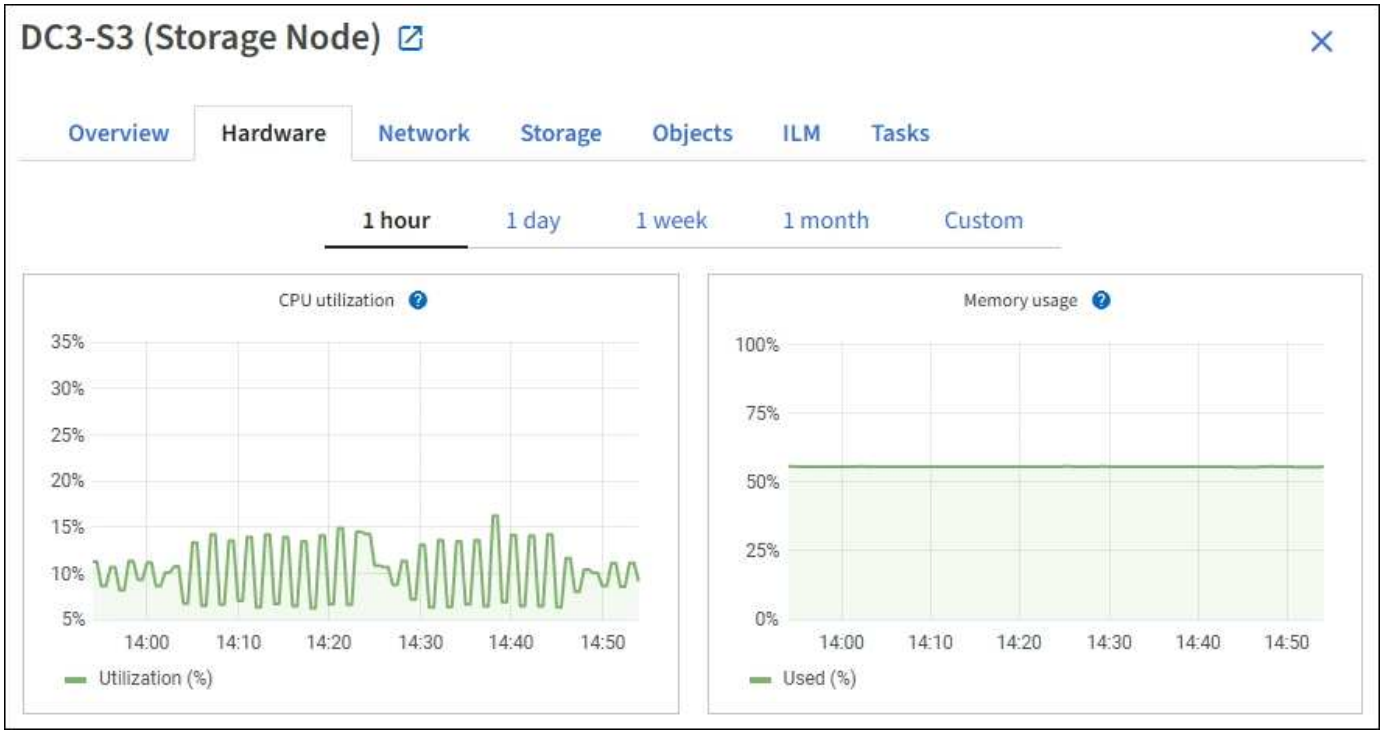
Alertas também estão incluídos para "estados de conexão do nó".

Veja a guia Hardware do StorageGRID

A aba Hardware exibe a utilização de CPU e o uso de memória para cada nó, além de informações adicionais sobre o hardware dos appliances.

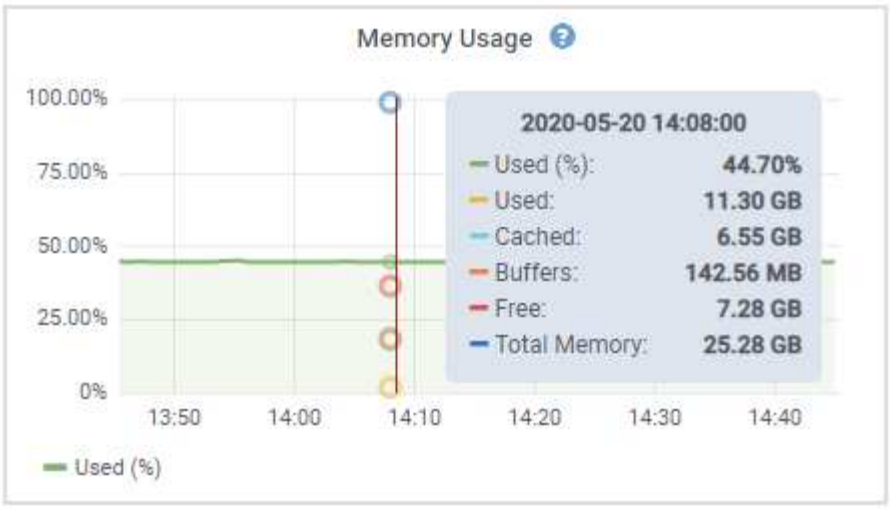
> O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A aba Hardware é exibida para todos os nós.



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

Para visualizar detalhes sobre a utilização de CPU e o uso de memória, posicione o cursor sobre cada gráfico.



Se o nó for um nó de appliance, esta aba também inclui uma seção com mais informações sobre o hardware do appliance.

Veja informações sobre Storage Nodes de dispositivos

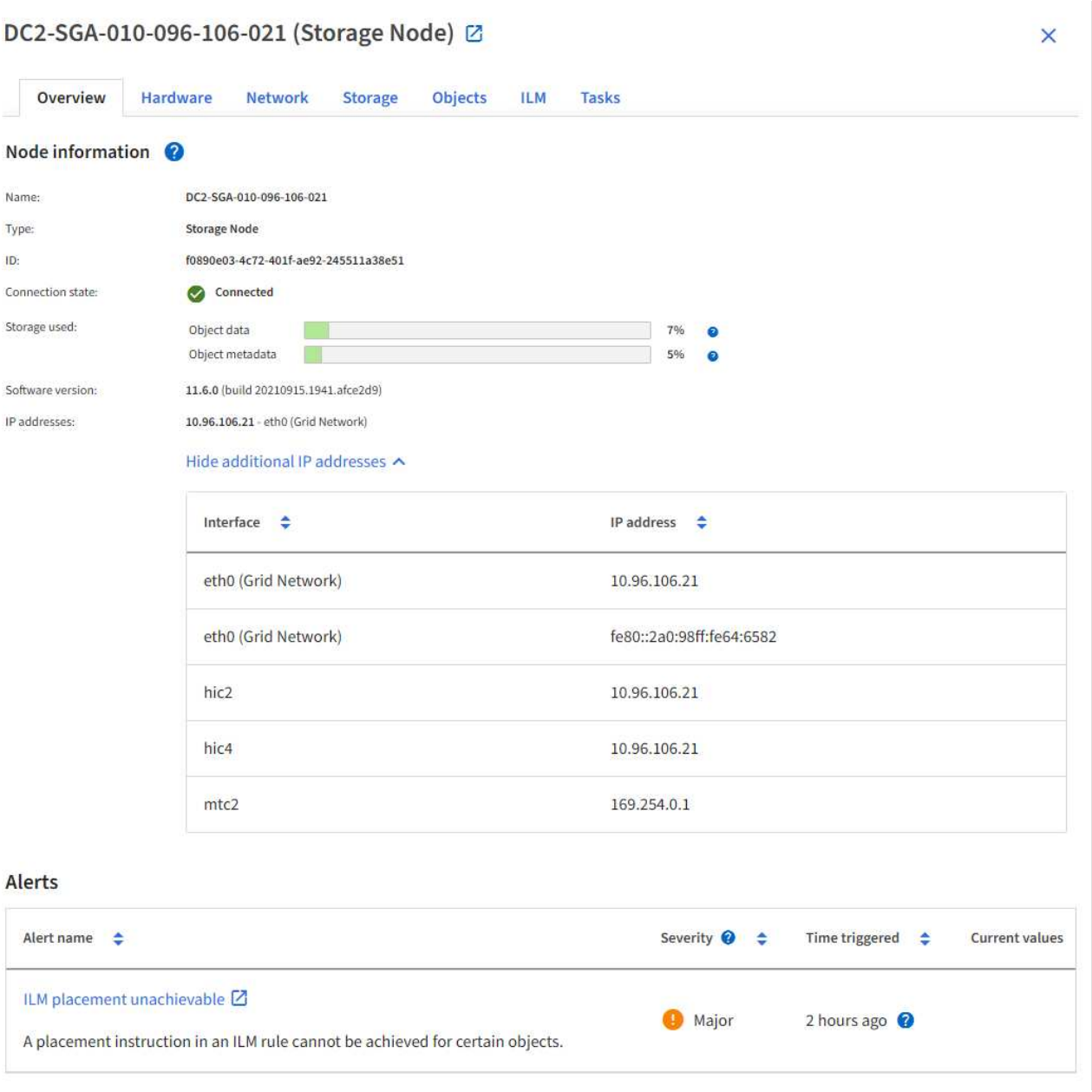
A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivos de disco e de rede para cada Storage Node do appliance. Você também pode visualizar memória, hardware de armazenamento, versão do firmware do controlador, recursos de rede, interfaces de rede, endereços de rede e dados recebidos e transmitidos.

Passos

1. Na página Nós, selecione um Storage Node do appliance.
2. Selecione **Visão geral**.

   A seção Informações do Nó na guia Visão Geral exibe informações resumidas sobre o nó, como o nome, tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, conforme a seguir:

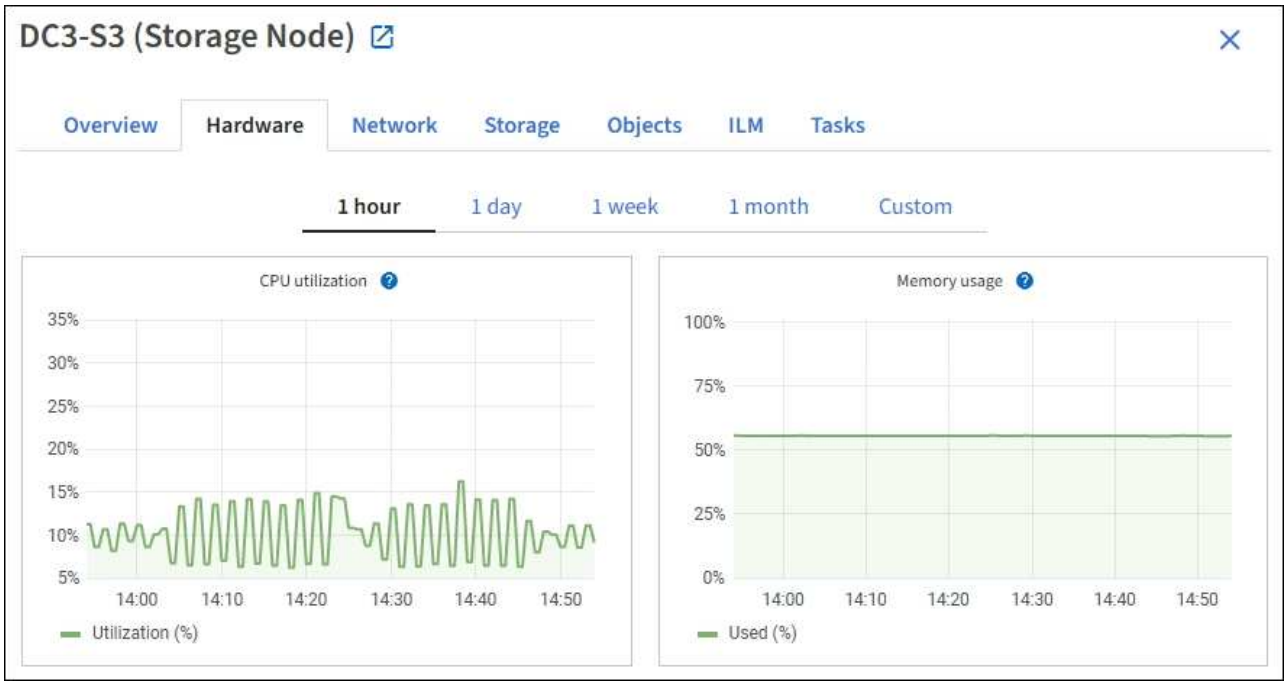
   - **eth**: a Grid Network, Admin Network ou Client Network.
   - **hic**: Uma das portas físicas de 10, 25 ou 100 GbE no appliance. Essas portas podem ser agregadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
   - **mtc**: Uma das portas físicas de 1 GbE no dispositivo.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



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

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

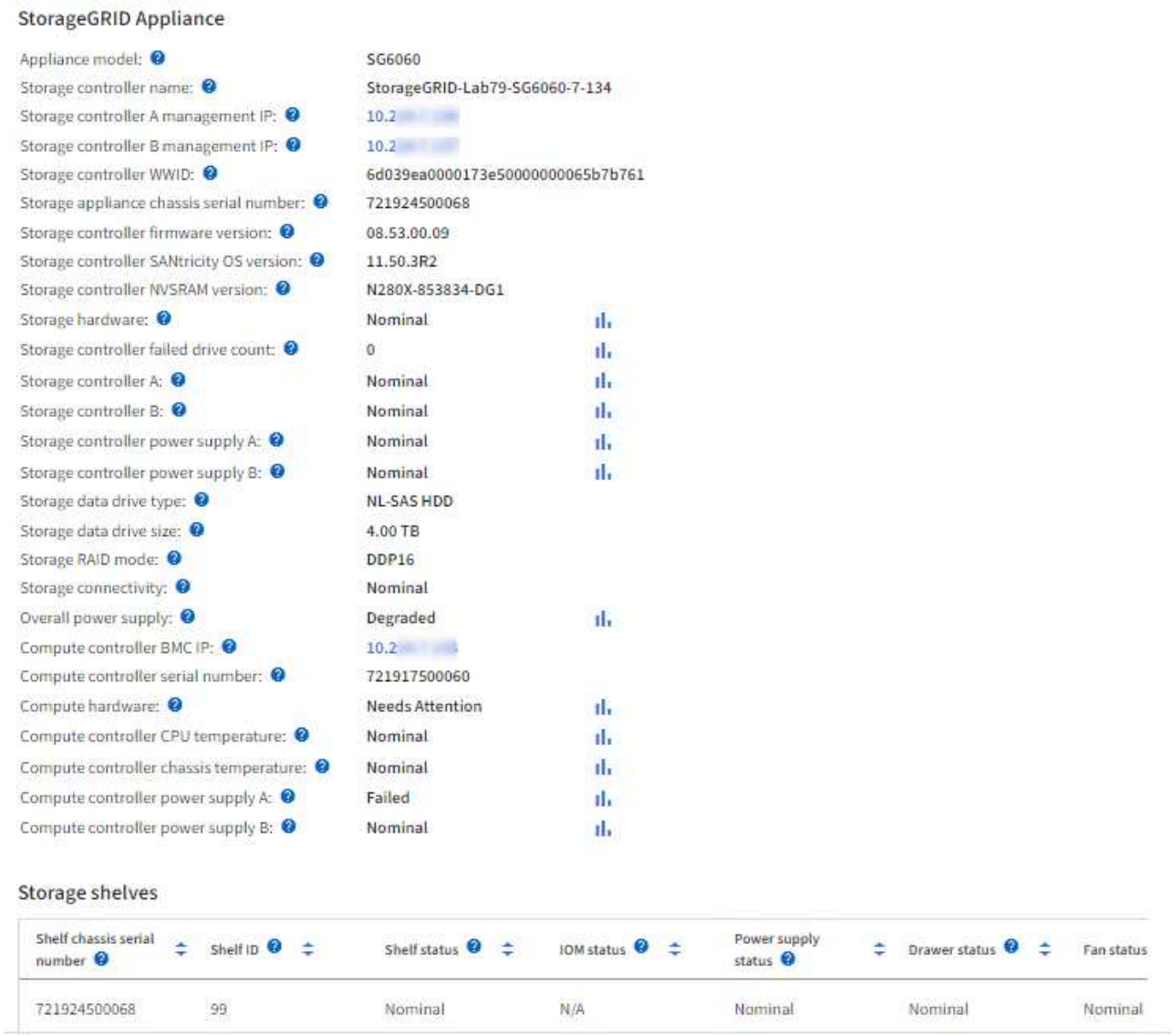
   a. Visualize os gráficos de utilização de CPU e memória para determinar as porcentagens de uso da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia,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



b. Deslize a tela para baixo para visualizar a tabela de componentes do appliance. Esta tabela contém informações como o nome do modelo do appliance; nomes dos controladores, números de série e endereços IP; e o status de cada componente.

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

Os componentes para as prateleiras de armazenamento e para as prateleiras de expansão, caso façam parte da instalação, aparecem em uma tabela separada abaixo da tabela do appliance.



Campo na tabela de Appliance	Descrição
Modelo do appliance	O número do modelo deste appliance StorageGRID exibido no SANtricity OS.
Nome do controlador de armazenamento	O nome deste appliance StorageGRID exibido no SANtricity OS.
IP de gerenciamento do controlador de armazenamento A	Endereço IP da porta de gerenciamento 1 no controlador de armazenamento A. Você usa esse IP para acessar SANtricity OS para solucionar problemas de armazenamento.
IP de gerenciamento do controlador de armazenamento B	Endereço IP da porta de gerenciamento 1 no controlador de armazenamento B. Você usa esse IP para acessar SANtricity OS para solucionar problemas de armazenamento. Alguns modelos de appliance não possuem um controlador de armazenamento B.

Campo na tabela de Appliance	Descrição
WWID do controlador de armazenamento	O identificador mundial do controlador de armazenamento exibido no SANtricity OS.
Número de série do chassi do appliance de armazenamento	O número de série do chassi do appliance.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento deste appliance.
Versão do sistema operacional SANtricity do controlador de armazenamento	A versão do SANtricity OS do controlador de armazenamento A.
Versão NVSRAM do controlador de armazenamento	Versão NVSRAM do controlador de armazenamento conforme relatado pelo SANtricity System Manager. Para os controladores SG6060 e SG6160, se houver uma incompatibilidade de versão da NVSRAM entre os dois controladores, a versão do controlador A é exibida. Se o controlador A não estiver instalado ou operacional, a versão do controlador B é exibida.
Hardware de armazenamento	O status geral do hardware do controlador de armazenamento. Se SANtricity System Manager reportar o status "Necessita de Atenção" para o hardware de armazenamento, o sistema StorageGRID também reportará esse valor. Se o status for "requer atenção", verifique primeiro o controlador de armazenamento usando SANtricity OS. Em seguida, certifique-se de que não existam outros alertas relacionados ao controlador de computação.
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não estão otimizadas.
Controlador de armazenamento A	O status do controlador de armazenamento A.
Controlador de armazenamento B	Status do controlador de armazenamento B. Alguns modelos de appliance não possuem um controlador de armazenamento B.
Fonte de alimentação do controlador de armazenamento A	Status da fonte de alimentação A para o controlador de armazenamento.
Fonte de alimentação do controlador de armazenamento B	Status da fonte de alimentação B para o controlador de armazenamento.

Campo na tabela de Appliance	Descrição
Tipo de unidade de armazenamento de dados	O tipo de unidade no appliance, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados. Para o SG6160, o tamanho da unidade de cache também é exibido. **Nota**: Para nós com compartimentos de expansão, use o Tamanho da unidade de dados para cada compartimento em vez disso. O tamanho efetivo da unidade pode variar de acordo com o compartimento.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de armazenamento	O estado da conectividade de armazenamento.
Fonte de alimentação geral	O status de todas as fontes de alimentação do appliance.
Endereço IP do BMC do controlador de computação	O endereço IP da porta do controlador de gerenciamento da placa-mãe (BMC) no controlador de computação. Você usa esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do appliance. Este campo não é exibido para modelos de appliance 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. Este campo não é exibido para modelos de dispositivos que não possuem 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.

+

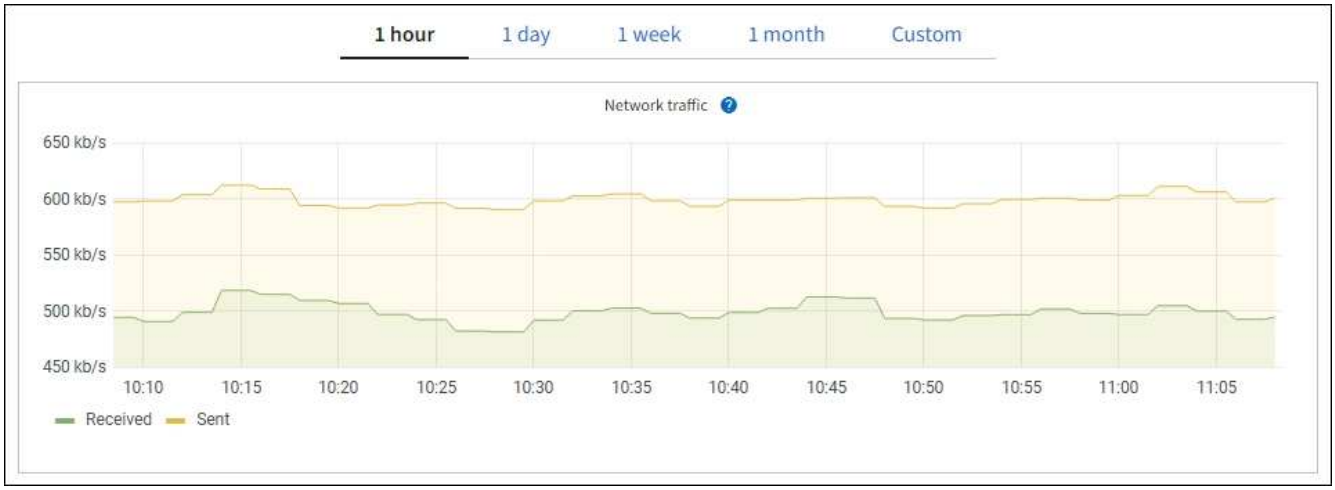
Coluna na tabela de compartimentos de armazenamento	Descrição
Número de série do chassi da prateleira	O número de série do chassi do compartimento de armazenamento.
ID do compartimento	O identificador numérico do compartimento de armazenamento. • 99: Prateleira do controlador de armazenamento • 0: Primeiro compartimento de expansão • 1: Segundo compartimento de expansão **Nota:** Compartimentos de expansão aplicam-se apenas ao SG6060 e SG6160.
Status do compartimento	Status geral do compartimento de armazenamento.
Status do IOM	O status dos módulos de entrada/saída (IOMs) em quaisquer compartimentos de expansão. N/A se não for um compartimento de expansão.
Status da fonte de alimentação	O status geral das fontes de alimentação do compartimento de expansão.
Status da gaveta	Status das gavetas no compartimento de armazenamento. N/A se o compartimento não contiver gavetas.
Status da ventoinha	O status geral das ventoinhas de refrigeração no compartimento de armazenamento.
Slots de unidade	O número total de slots para unidades no compartimento de armazenamento.
Unidades de dados	O número de unidades no compartimento de armazenamento que são usadas para storage de dados.
Tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados no compartimento de armazenamento.
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, todas as unidades de cache têm o mesmo tamanho.
Estado da configuração	O status de configuração do compartimento de armazenamento.

a. Confirme se todos os status estão como "Nominal".

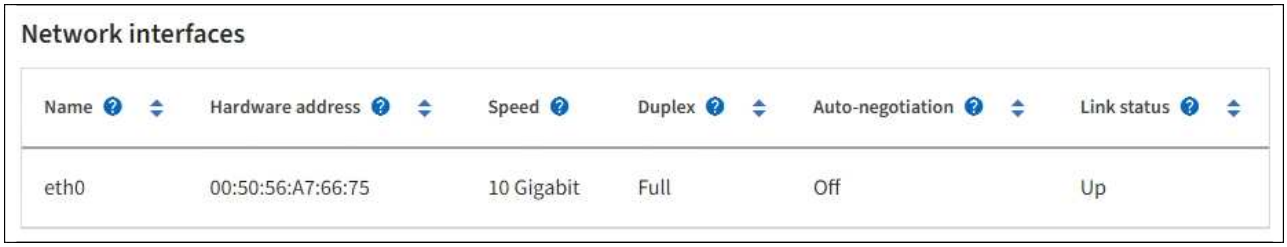
   Se o status não for "Nominal", verifique os alertas atuais. Você também pode usar SANtricity System Manager para saber mais sobre alguns desses valores de hardware. Consulte as instruções para instalar e manter seu appliance.

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

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



a. Revise a seção 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

   Utilize a tabela a seguir com os valores da coluna **Velocidade** na tabela Interfaces de Rede para determinar se as portas de rede 10/25-GbE do appliance foram configuradas para usar o modo ativo/backup ou o modo LACP.

   Os valores apresentados na tabela pressupõem que todos os quatro links sejam utilizados.

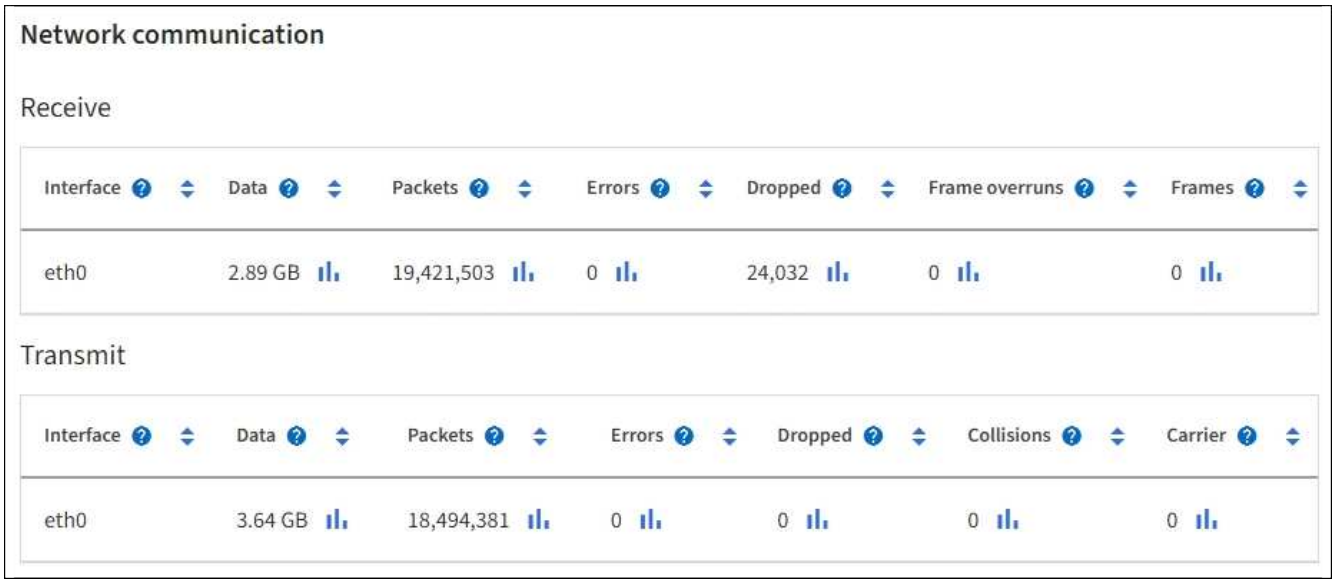
Modo de link	Modo bond	Velocidade individual do link HIC (hic1, hic2, hic3, hic4)	Velocidade esperada da rede Grid/cliente (eth0,eth2)
Agregado	LACP	25	100
Fixo	LACP	25	50
Fixo	Ativo/Backup	25	25

Modo de link	Modo bond	Velocidade individual do link HIC (hic1, hic2, hic3, hic4)	Velocidade esperada da rede Grid/cliente (eth0,eth2)
Agregado	LACP	10	40
Fixo	LACP	10	20
Fixo	Ativo/Backup	10	10

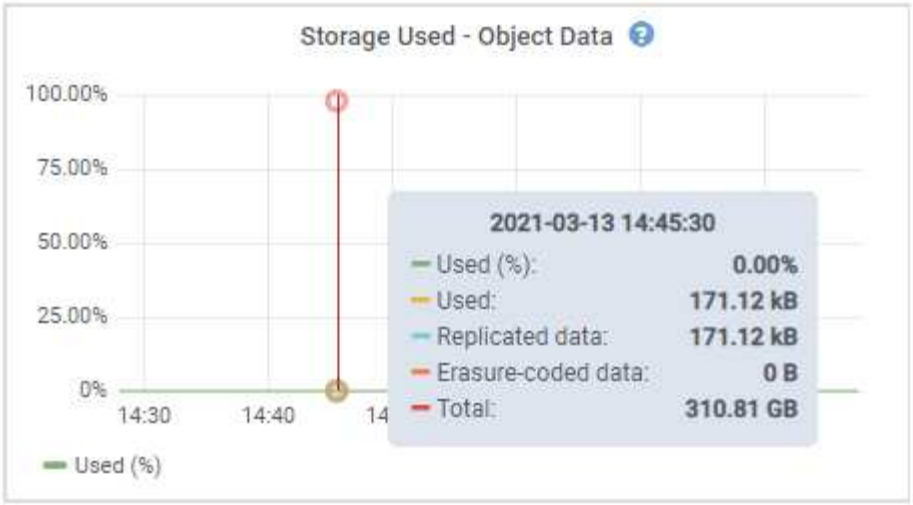
Consulte "Configurar links de rede" para obter mais informações sobre como configurar as portas 10/25-GbE.

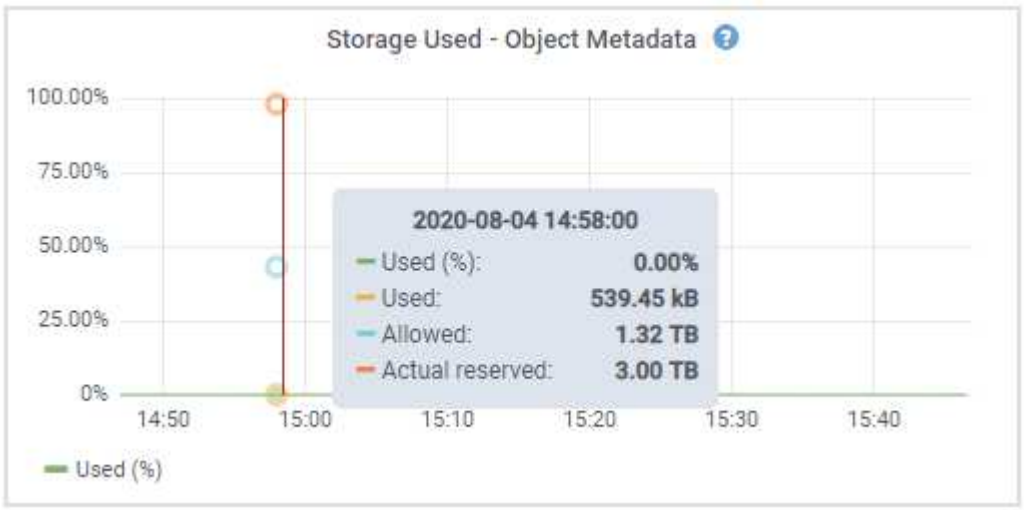
b. Revise a seção Comunicação em Rede.

As tabelas de Recebimento e Transmissão mostram quantos bytes e pacotes foram recebidos e enviados em cada rede, assim como outras métricas de recebimento e transmissão.



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

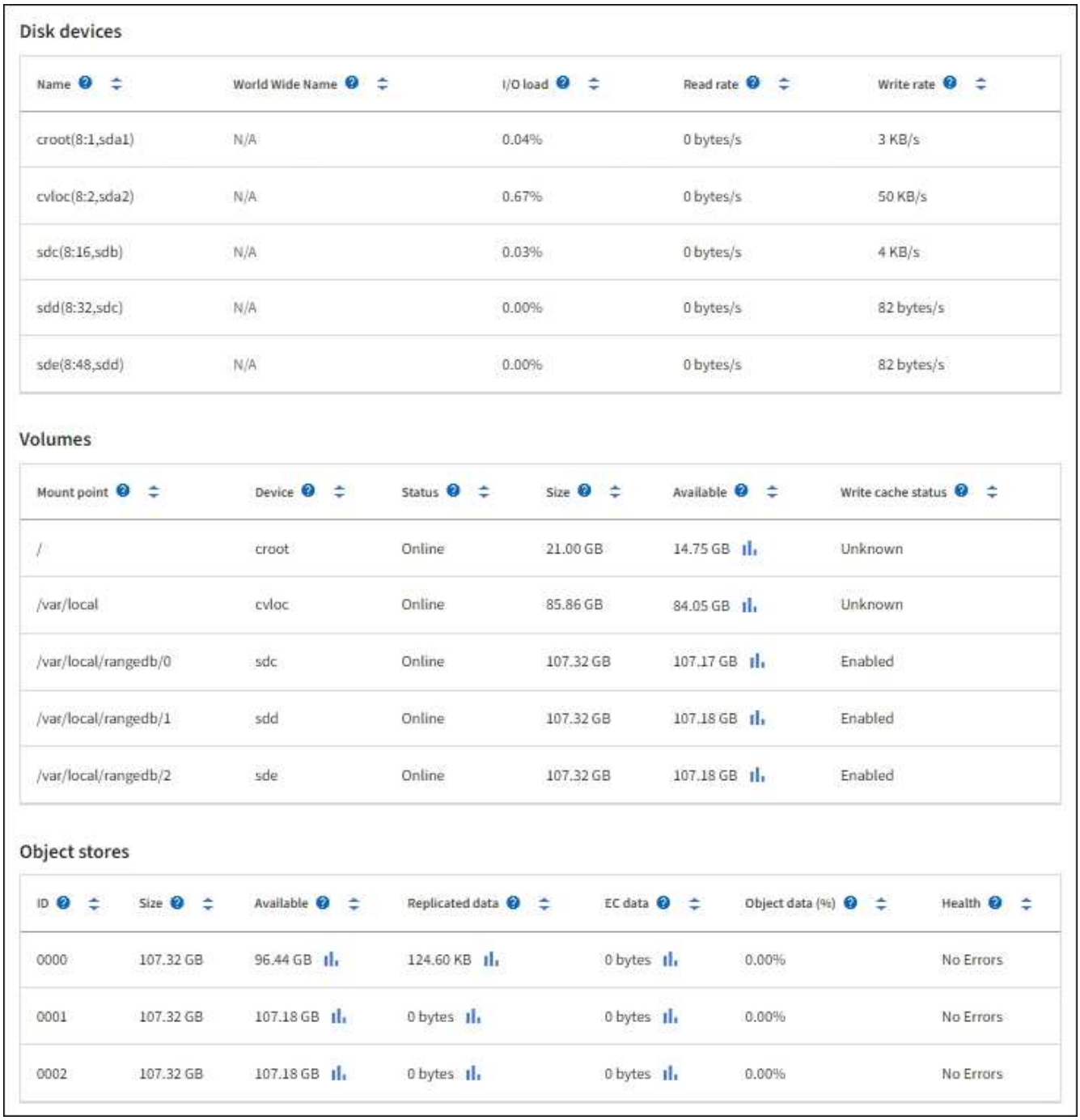




a. Deslize a tela para baixo para visualizar as quantidades de espaço de storage disponíveis para cada volume e armazenamento de objetos.

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

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



Veja informações sobre os nós de administração e os nós de gateway do appliance

A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivos de disco e de rede para cada appliance de serviços usado como Admin Node ou Gateway Node. Você também pode visualizar memória, hardware de storage, recursos de rede, interfaces de rede, endereços de rede e dados de recebimento e transmissão.

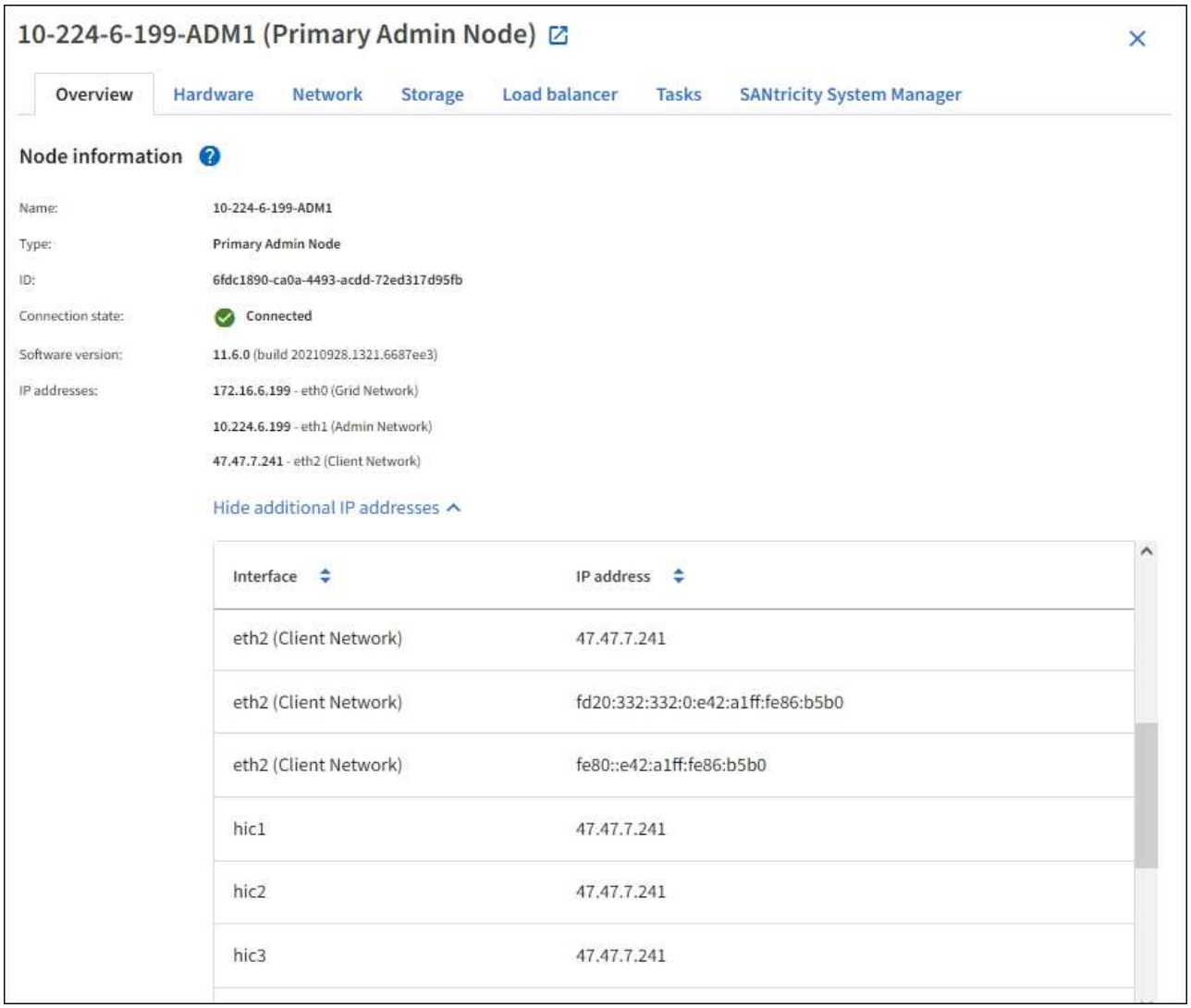
Passos

1. Na página Nós, selecione um appliance Admin Node ou um appliance Gateway Node.
2. Selecione **Visão geral**.

   A seção Informações do Nó na guia Visão Geral exibe informações resumidas sobre o nó, como o nome,

tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, conforme a seguir:

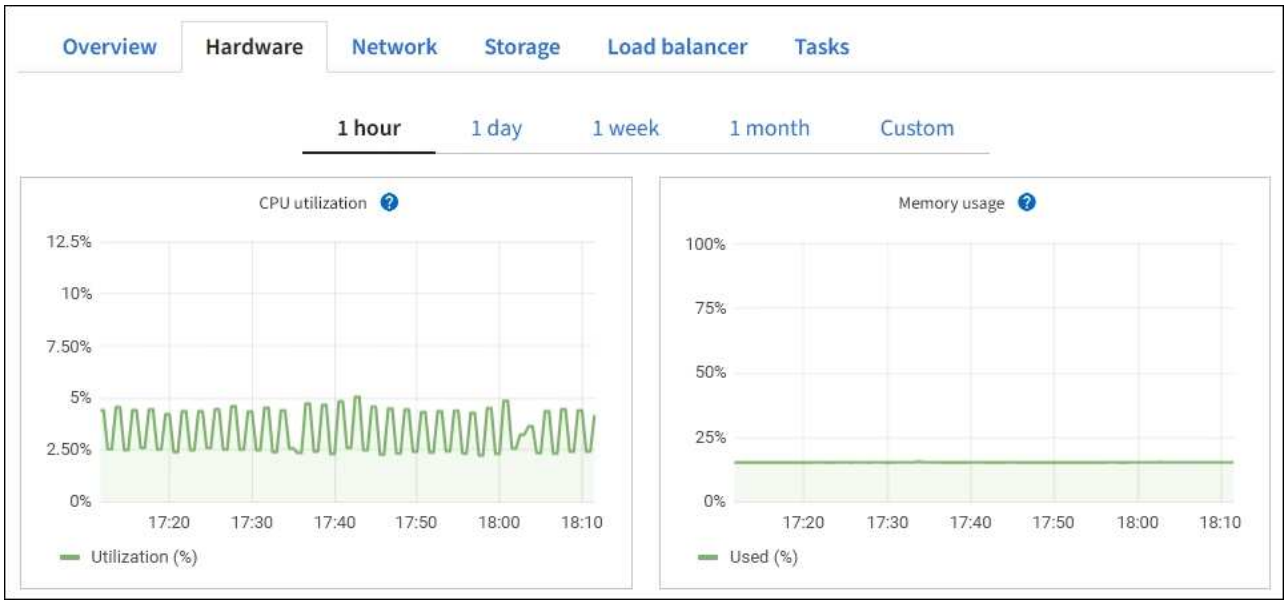
- **adllb** e **adlli**: exibidos se o vínculo ativo/backup estiver sendo usado para a interface da rede de administração
- **eth**: a Grid Network, Admin Network ou Client Network.
- **hic**: Uma das portas físicas de 10, 25 ou 100 GbE no appliance. Essas portas podem ser agregadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
- **mtc**: Uma das portas físicas de 1 GbE no appliance. Uma ou mais interfaces mtc são agregadas para formar a interface de rede Admin (eth1). Você pode deixar outras interfaces mtc disponíveis para conectividade local temporária para um técnico no data center.



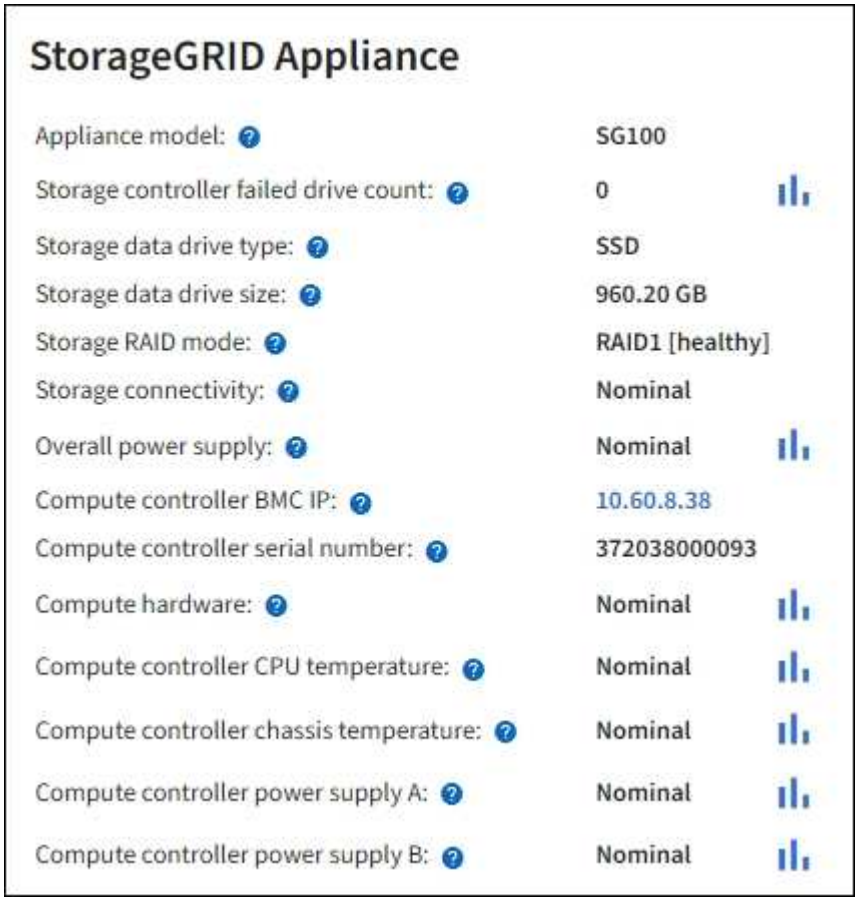
A seção Alertas da guia Visão geral exibe todos os alertas ativos para o nó.

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

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



b. Deslize a tela para baixo para visualizar a tabela de componentes do appliance. 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 tabela de Appliance	Descrição
Modelo do appliance	O número do modelo deste appliance StorageGRID.

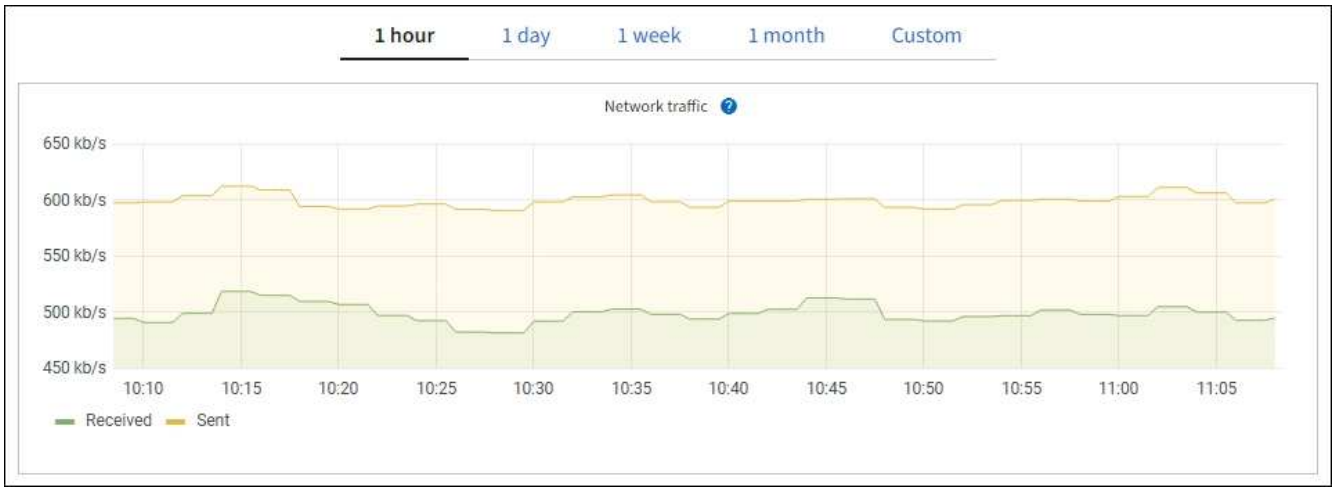
Campo na tabela de Appliance	Descrição
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não estão otimizadas.
Tipo de unidade de armazenamento de dados	O tipo de unidade no appliance, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados.
Modo RAID de armazenamento	O modo RAID para o dispositivo.
Fonte de alimentação geral	O status de todas as fontes de alimentação do appliance.
Endereço IP do BMC do controlador de computação	O endereço IP da porta do controlador de gerenciamento da placa-mãe (BMC) no controlador de computação. Você pode usar esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do appliance. Este campo não é exibido para modelos de appliance 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. Confirme se todos os status estão como "Nominal".

   Se o status não for "Nominal", verifique os alertas atuais.

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

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



a. Revise a seção Interfaces de Rede.

Network interfaces

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

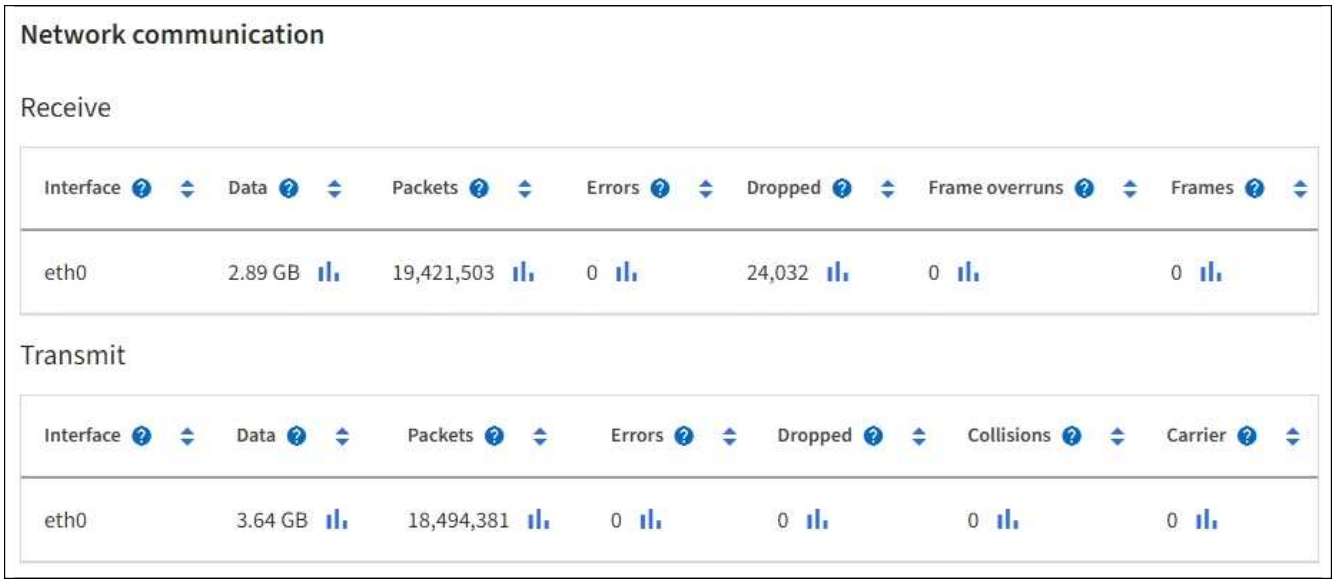
Utilize a tabela a seguir com os valores da coluna **Velocidade** na tabela Interfaces de Rede para determinar se as quatro portas de rede 40/100-GbE do appliance foram configuradas para usar o modo ativo/backup ou o modo LACP.

Os valores apresentados na tabela pressupõem que todos os quatro links sejam utilizados.

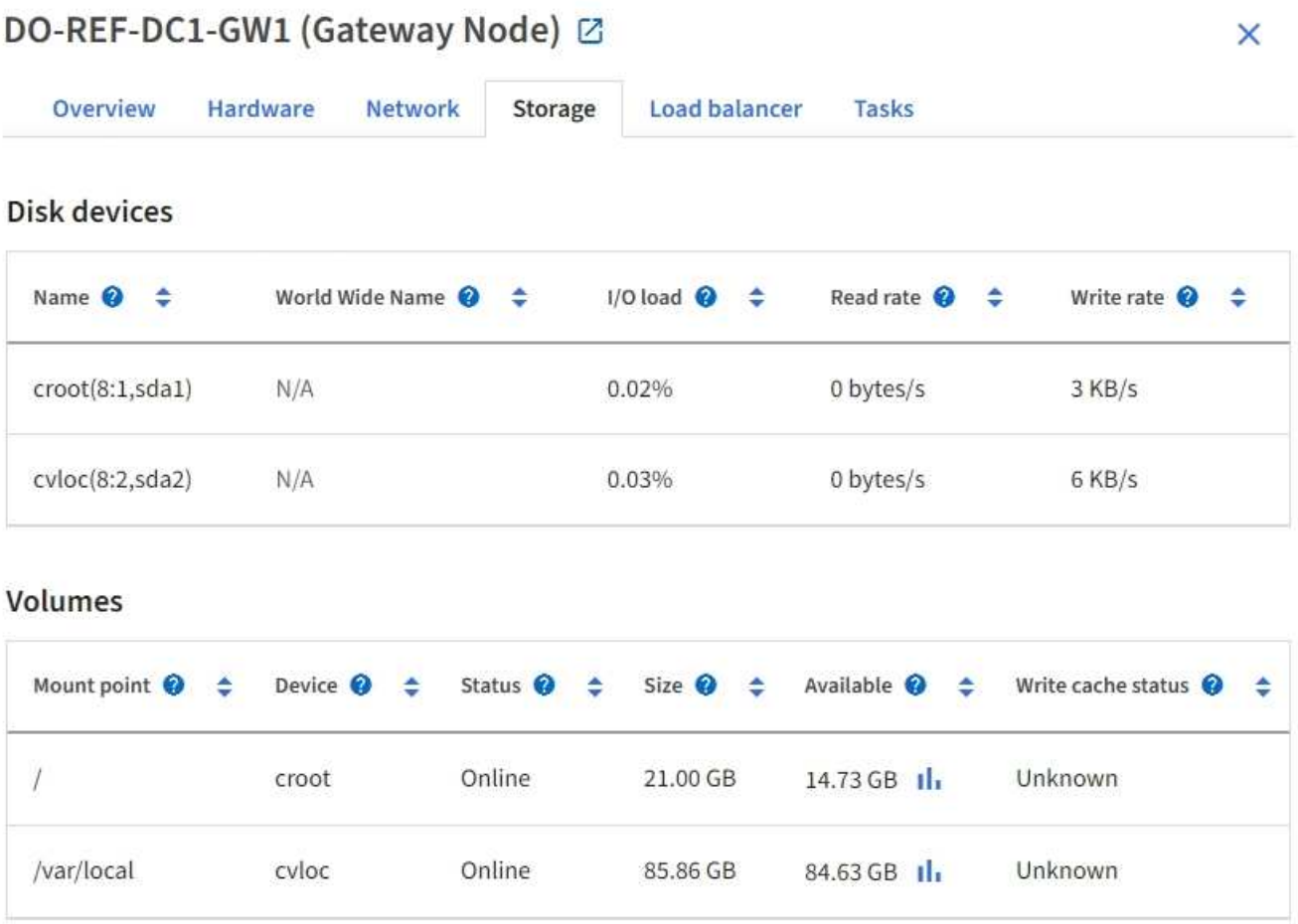
Modo de link	Modo bond	Velocidade individual do link HIC (hic1, hic2, hic3, hic4)	Velocidade esperada da rede Grid/cliente (eth0, eth2)
Agregado	LACP	100	400
Fixo	LACP	100	200
Fixo	Ativo/Backup	100	100
Agregado	LACP	40	160
Fixo	LACP	40	80
Fixo	Ativo/Backup	40	40

b. Revise a seção Comunicação em Rede.

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



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



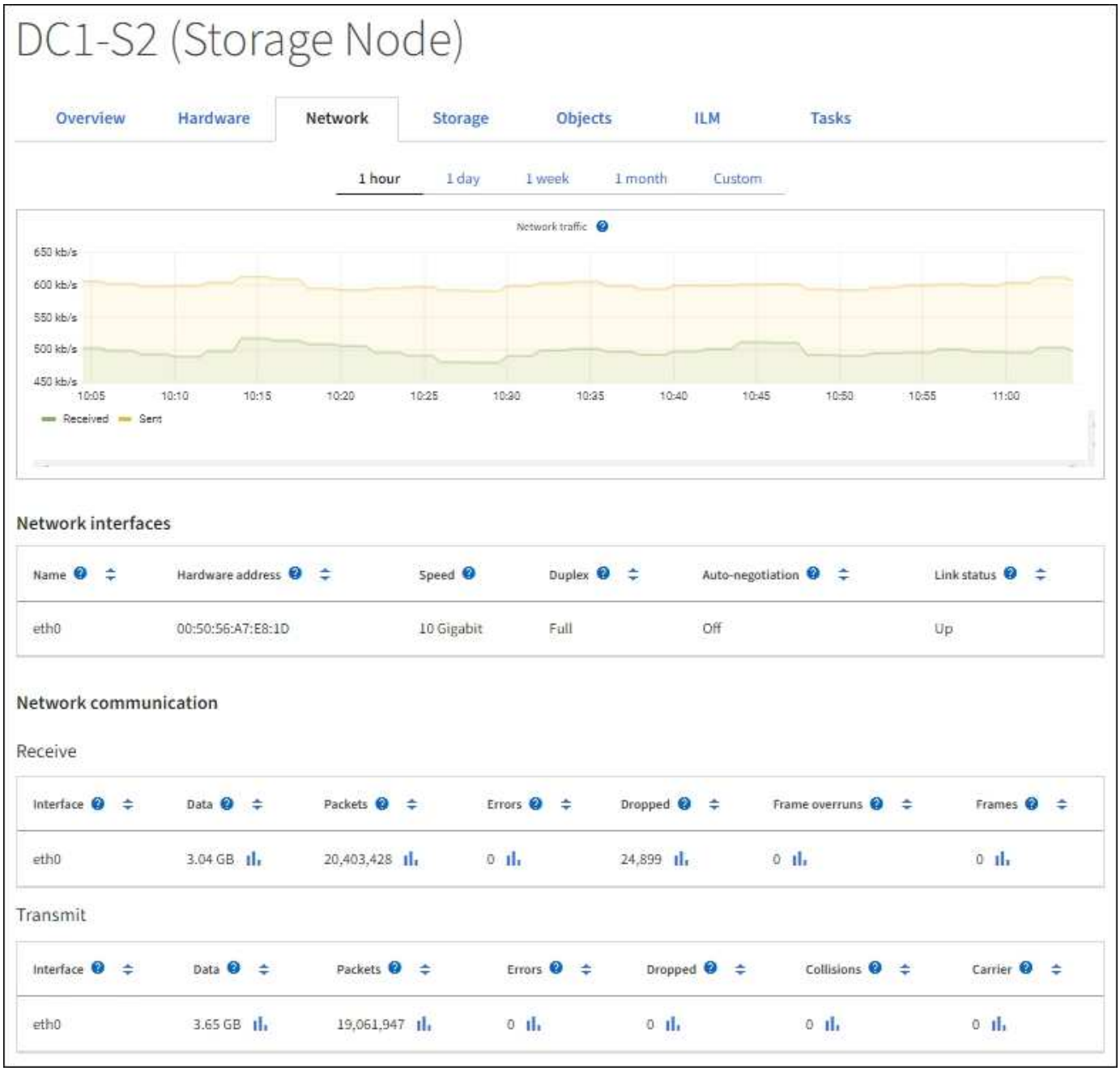
Visualize a guia Rede do StorageGRID

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

A aba Rede é exibida para todos os nós, cada site e toda a grid.

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

Para os nós, a tabela Interfaces de Rede fornece informações sobre as portas de rede físicas de cada nó. A tabela Comunicações de Rede fornece detalhes sobre as operações de recebimento e transmissão de cada nó e quaisquer contadores de falhas relatados pelo driver.



Informações relacionadas

"Monitore as conexões de rede e o desempenho"

Visualize a guia Storage do StorageGRID

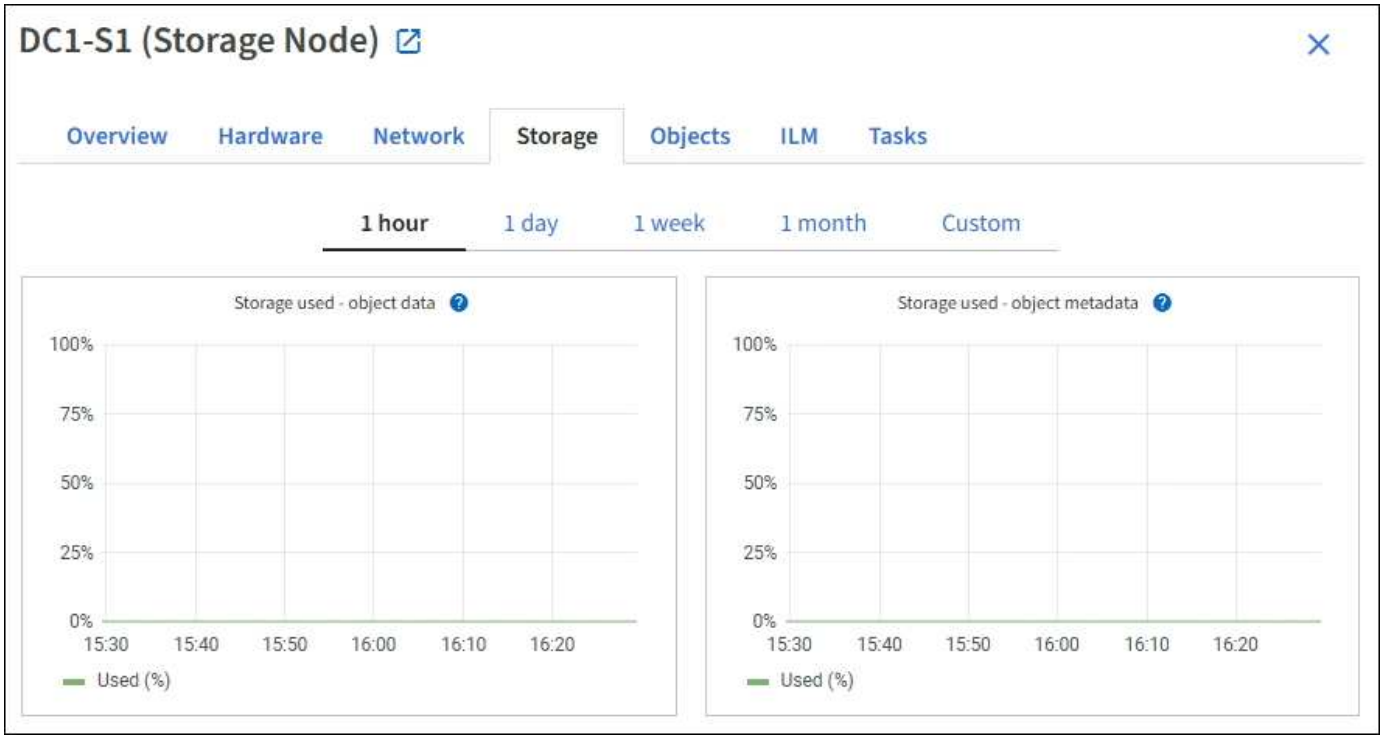
A aba Armazenamento resume a disponibilidade de storage e outras métricas de storage.

A aba Storage é exibida para todos os nós, cada site e toda a grid.

Gráficos de armazenamento usado

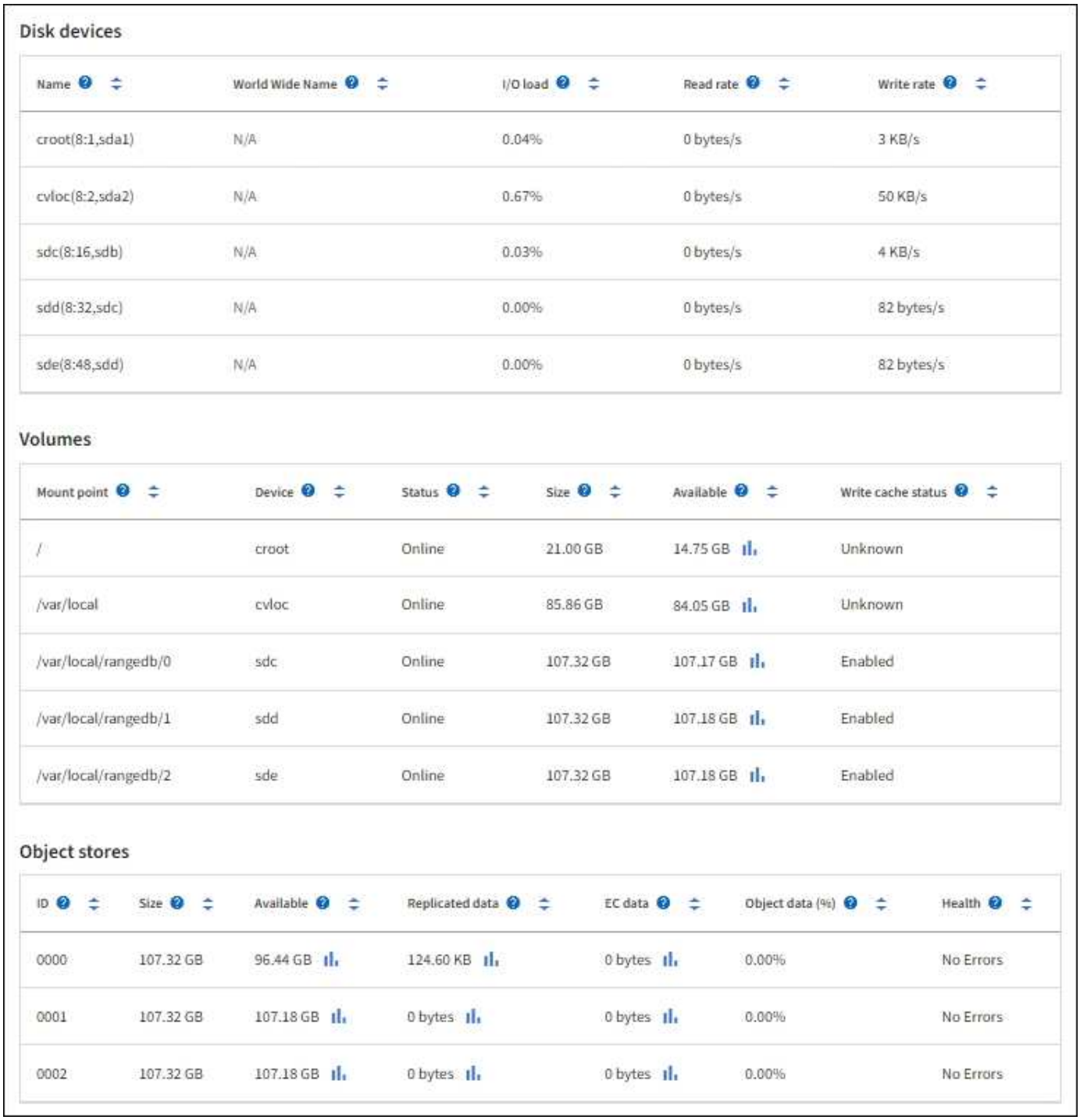
Para os nós de armazenamento, cada site e toda a grid, a guia Armazenamento inclui gráficos que mostram quanto storage foi usado pelos dados de objeto e metadados de objeto ao longo do tempo.

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



Tabelas de dispositivos de disco, volumes e object stores

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



Disk devices

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

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

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

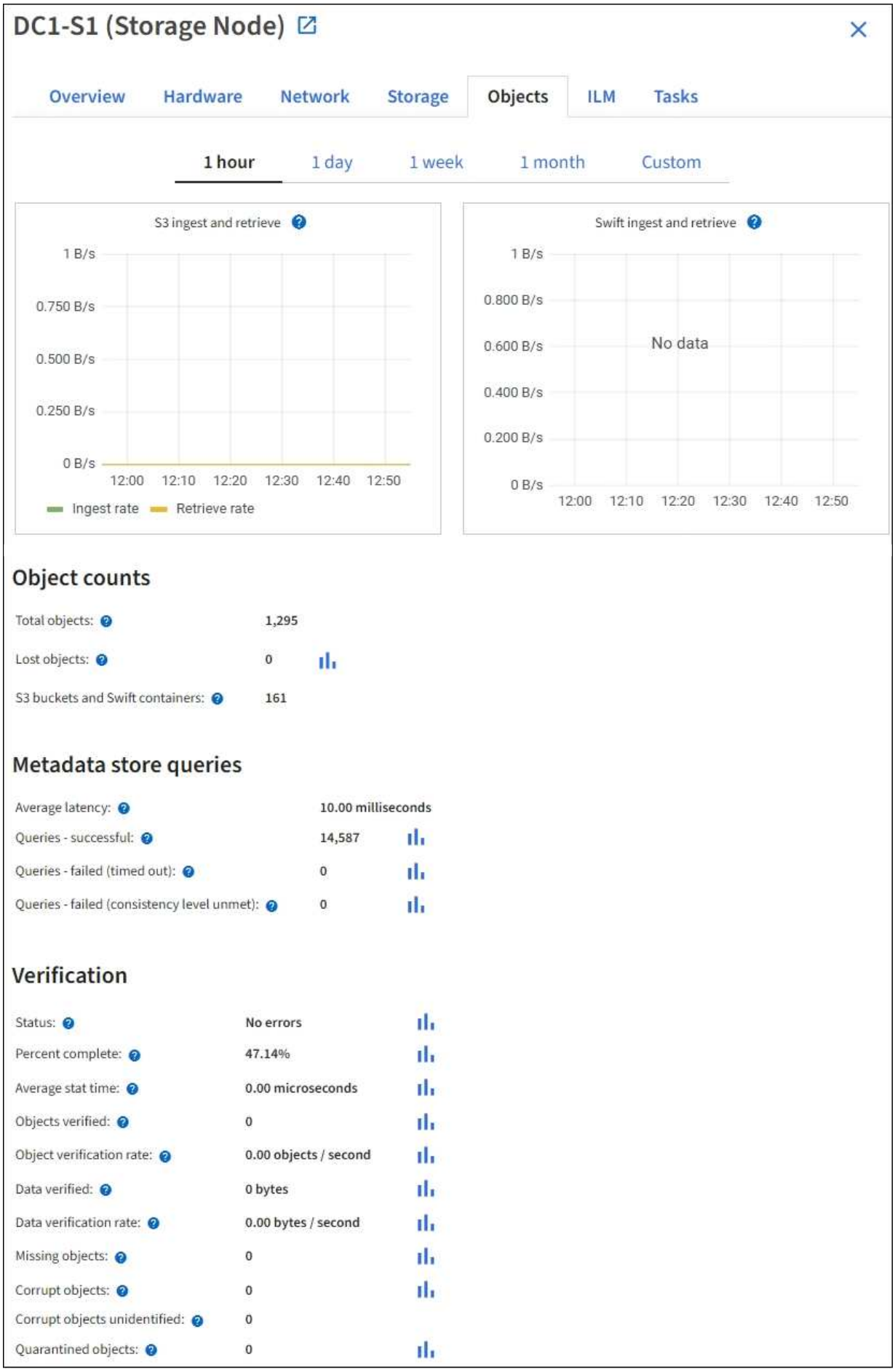
Informações relacionadas

"Monitorar a capacidade de storage"

Visualize a guia Objetos do StorageGRID

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

A aba Objetos é exibida para cada Storage Node, cada site e toda a grid. Para Storage Nodes, a aba Objetos também fornece contagens de objetos e informações sobre consultas de metadados e verificação em segundo plano.

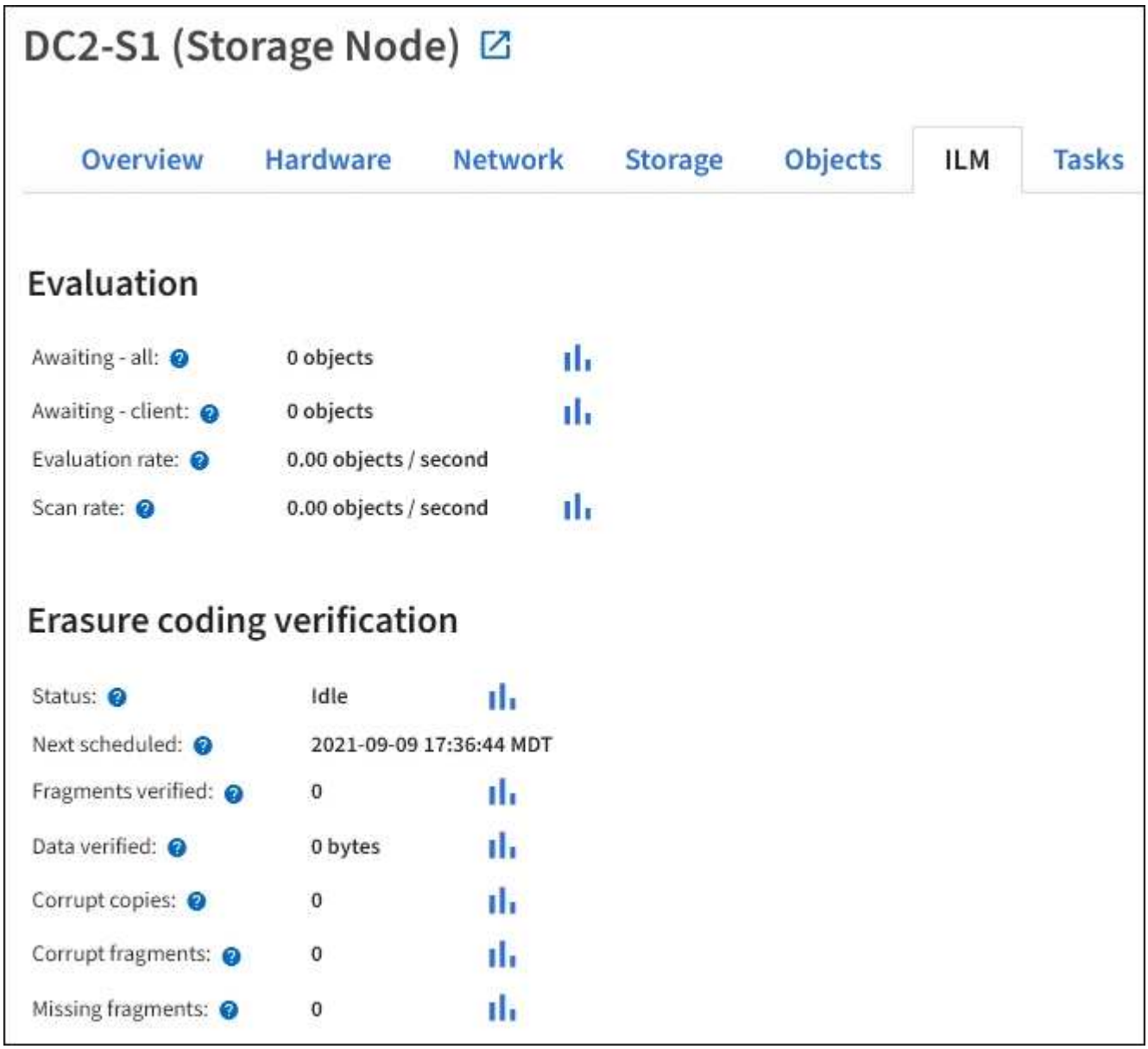

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

Visualize a guia StorageGRID ILM

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

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

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



Informações relacionadas

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

Visualize a guia Load balancer do StorageGRID

A aba Balanceador de Carga inclui gráficos de desempenho e diagnóstico relacionados à operação do serviço Load Balancer.

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

Se não houver nenhuma operação de E/S sendo executada pelo serviço de balanceador de carga, ou se nenhum balanceador de carga estiver configurado, os gráficos exibem "Sem dados".

Tráfego de solicitação

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

Esse valor é atualizado ao término de cada solicitação. Como resultado, esse valor pode diferir da taxa de transferência em tempo real em baixas taxas de requisição ou para requisições de longa duração. Você pode consultar a aba Rede para obter uma visão mais realista do comportamento atual da rede.

Taxa de solicitações recebidas

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

Duração média da solicitação (sem erro)

Este gráfico fornece uma média móvel de 3 minutos da duração das requisições, discriminada por tipo de requisição (GET, PUT, HEAD e DELETE). A duração de cada requisição começa quando o cabeçalho da requisição é analisado pelo serviço Load Balancer e termina quando o corpo completo da resposta é retornado ao cliente.

Taxa de resposta de erro

Este gráfico apresenta a média móvel de 3 minutos do número de respostas de erro retornadas aos clientes por segundo, discriminadas pelo código de resposta de erro.

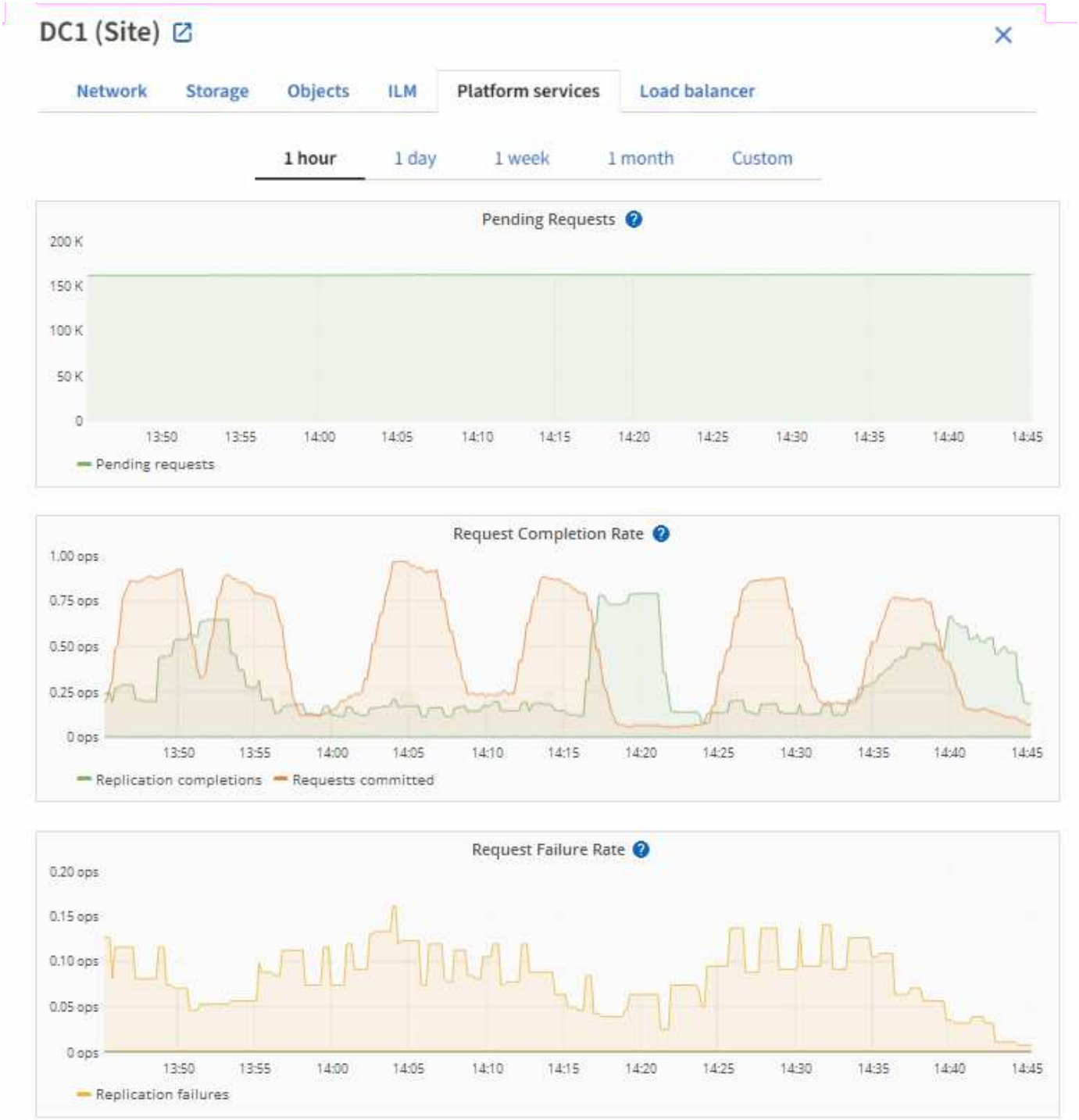
Informações relacionadas

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

Veja a aba de serviços da plataforma StorageGRID

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

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



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

Visualize a guia Gerenciar unidades do StorageGRID

A guia Gerenciar unidades permite que você acesse detalhes e execute tarefas de solução de problemas e manutenção em unidades nos appliances que suportam esse recurso.

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

- Veja um layout das storage drives de dados no appliance
- Veja uma tabela que lista a localização, o tipo, o status, a versão do firmware e o número de série de cada unidade
- Execute funções de diagnóstico e manutenção em cada drive

Para acessar a guia Gerenciar unidades, você precisa ter o "Permissão de administrador do dispositivo de storage ou acesso root".

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

Visualize a guia SANtricity System Manager do StorageGRID

A aba SANtricity System Manager permite que você acesse o SANtricity System Manager sem precisar configurar ou conectar a porta de gerenciamento do dispositivo de storage. Você pode usar esta aba para revisar informações de diagnóstico de hardware e ambientais, assim como questões relacionadas às unidades.

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

> A guia SANtricity System Manager é exibida apenas para nós de dispositivo de storage que utilizam hardware E-Series.

Utilizando SANtricity System Manager, você pode fazer o seguinte:

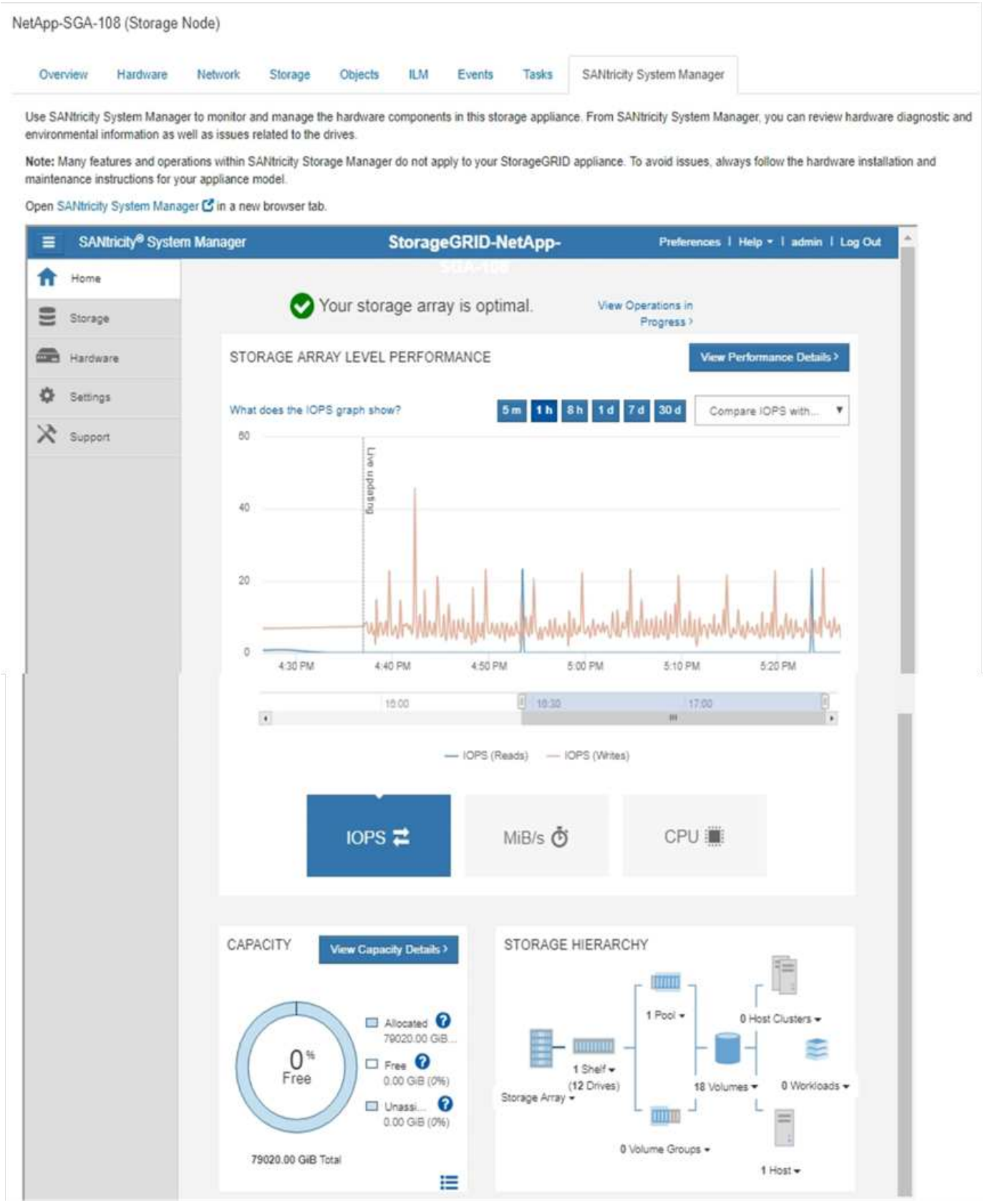
- Visualize dados de desempenho, como desempenho em nível de array de storage, latência de I/O, utilização de CPU do controlador de storage e taxa de transferência.
- Verifique o status dos componentes de hardware.
- Execute funções de suporte, incluindo a visualização de dados de diagnóstico e a configuração do E-Series AutoSupport.

> Para usar SANtricity System Manager para configurar um proxy para E-Series AutoSupport, consulte "Envie pacotes E-Series AutoSupport através do StorageGRID".

Para acessar SANtricity System Manager através do Grid Manager, você precisa ter o "Permissão de administrador do dispositivo de storage ou acesso root".

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

A aba exibe a página inicial do SANtricity System Manager.



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

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

cada gráfico.

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

Informações para monitorar regularmente

O que e quando monitorar no StorageGRID

Embora o sistema StorageGRID possa continuar operando quando ocorrem erros ou partes da grid estão indisponíveis, você deve monitorar e solucionar possíveis problemas antes que eles afetem a eficiência ou a disponibilidade da grid.

Antes de começar

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

Sobre tarefas de monitoramento

Um sistema em alta demanda gera grandes quantidades de informações. A lista a seguir fornece orientações sobre as informações mais importantes a serem monitoradas continuamente.

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

Monitore a integridade do sistema no StorageGRID

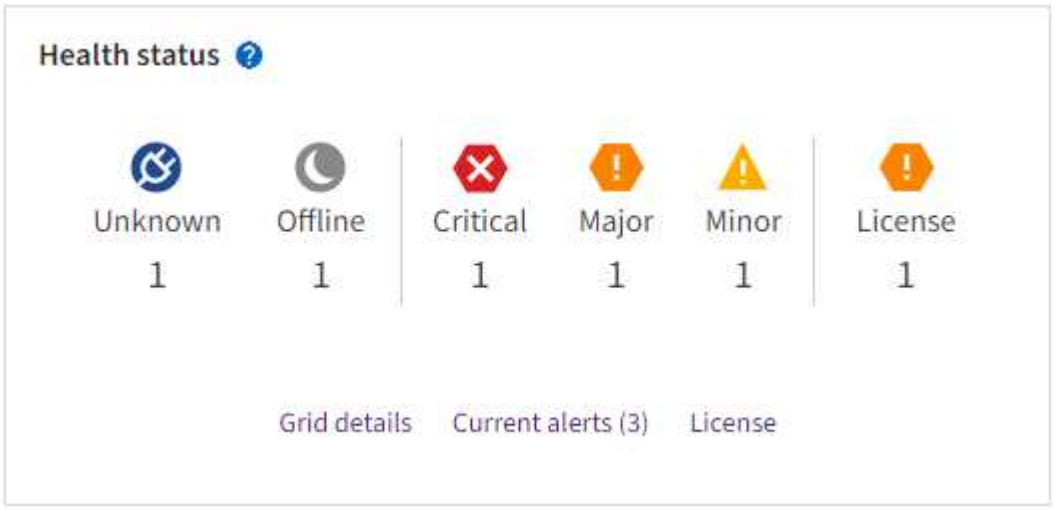
Monitore diariamente a saúde geral do seu sistema StorageGRID.

Sobre esta tarefa

O sistema StorageGRID pode continuar operando quando partes do grid estiverem indisponíveis. Problemas potenciais indicados por alertas não são necessariamente problemas nas operações do sistema. Investigue os

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

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



Quando surgirem problemas, aparecerão links que permitem que você visualize detalhes adicionais:

Link	Aparece quando…
Detalhes do grid	Quaisquer nós estão desconectados (estado da conexão Desconhecido ou Administrativamente Down).
Alertas atuais (Crítico, Grave, Leve)	Os alertas são atualmente ativo.
Alertas resolvidos recentemente	Alertas acionados na última semana agora estão resolvidos.
Licença	Existe um problema com a licença de software deste sistema StorageGRID. Você pode "Atualize as informações da licença conforme necessário".

Monitorar os estados de conexão dos nós

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

Ícone	Descrição	Ação necessária
	Não conectado - Desconhecido Por razões desconhecidas, um nó é desconectado ou os serviços no nó são interrompidos inesperadamente. Por exemplo, um serviço no nó pode ter sido interrompido ou o nó pode ter perdido a conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta **Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. Selecione cada alerta e siga as ações recomendadas. Por exemplo, você pode precisar reiniciar um serviço que parou ou reiniciar o host do nó. **Nota**: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	Sem conexão - administrativamente inativo Por um motivo previsível, o nó não está conectado à grid. Por exemplo, o nó, ou os serviços no nó, foi desligado corretamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Dependendo do problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Verifique se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos, selecione cada alerta siga as ações recomendadas.
	Conectado O nó está conectado à grid.	Nenhuma ação necessária.

Veja os 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 Nodes. Se "As notificações de alerta por e-mail 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:

Visão geral dos alertas

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

Cabeçalho da coluna	Descrição
Nome ou título	O nome do alerta e sua descrição.

Cabeçalho da coluna	Descrição
Gravidade	A gravidade do alerta. Para alertas atuais, se vários alertas estiverem agrupados, a linha de título mostra quantas ocorrências desse alerta estão acontecendo em cada nível de gravidade. **Crítico**: Existe uma condição anormal que interrompeu o funcionamento normal de um nó ou serviço do StorageGRID. Você deve resolver o problema imediatamente. A não resolução do problema pode resultar em interrupção do serviço e perda de dados. **Grave**: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar alertas graves e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um StorageGRID node ou serviço. **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se persistir. Você deve monitorar e resolver alertas menores que não se resolvem sozinhos para garantir que não resultem em um problema mais sério.
Acionado por tempo	**Alertas atuais**: A data e a hora em que o alerta foi acionado no seu horário local e em UTC. Se vários alertas estiverem agrupados, a linha de título mostra os horários da instância mais recente do alerta (*newest*) e da instância mais antiga do alerta (*oldest*). **Alertas resolvidos**: há quanto tempo o alerta foi acionado.
Site/Nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.
Status	Indica se o alerta está ativo, silenciado ou resolvido. Se vários alertas estiverem agrupados e a opção **Todos os alertas** estiver selecionada no menu suspenso, a linha do título mostra 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 acionou o alerta. Para alguns alertas, valores adicionais são exibidos para ajudar você a entender e investigar o alerta. Por exemplo, os valores exibidos para um alerta de **Low object data storage** incluem a porcentagem de espaço de disco usado, a quantidade total de espaço de disco e a quantidade de espaço de disco usado. **Nota:** Se vários alertas atuais estiverem agrupados, os valores atuais não são exibidos na linha de título.

Cabeçalho da coluna	Descrição
Valores acionados (somente alertas resolvidos)	O valor da métrica que acionou o alerta. Para alguns alertas, valores adicionais são exibidos para ajudar você a entender e investigar o alerta. Por exemplo, os valores exibidos para um alerta de **Low object data storage** incluem a porcentagem de espaço de disco usado, a quantidade total de espaço de disco e a quantidade de espaço de disco usado.

Passos

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

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

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

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

2. Para expandir grupos de alertas, selecione a seta para baixo . Para recolher alertas individuais em um grupo, selecione a seta para cima ou selecione o nome do grupo.
3. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **Agrupar alertas**.
4. Para classificar os alertas atuais ou grupos de alertas, selecione as setas para cima/para baixo em cada cabeçalho de coluna.
   - Quando a opção **Agrupar alertas** é selecionada, tanto os grupos de alertas quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **Hora de acionamento** para encontrar a instância mais recente de um alerta específico.
   - Quando a opção **Agrupar alertas** é desmarcada, 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**, **Ativos** ou **Silenciados**, use o menu suspenso na parte superior da tabela.

   Consulte "Silenciar notificações de alerta".

6. Para classificar os alertas resolvidos:
   - Selecione um período de tempo no menu suspenso **Quando acionado**.
   - Selecione uma ou mais gravidades no menu suspenso **Gravidade**.
   - Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **Regra de alerta** para filtrar alertas resolvidos relacionados a uma regra de alerta específica.
   - Selecione um ou mais nós no menu suspenso **Nó** para filtrar os alertas resolvidos relacionados a um

nó específico.

7. Para visualizar os detalhes de um alerta específico, selecione o alerta. Uma caixa de diálogo fornece detalhes e ações recomendadas para o alerta que você selecionou.
8. (Opcional) Para um alerta específico, selecione silenciar este alerta para silenciar a regra de alerta que fez com que este alerta fosse acionado.

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

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

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

      Aparece uma janela pop-up, listando a expressão Prometheus para cada nível de severidade definido.

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

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

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

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

Monitore a capacidade de storage no StorageGRID

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

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

Você pode "visualizar informações sobre a capacidade de storage" para toda a grid, para cada site e para cada Storage Node no seu sistema StorageGRID.

Monitorar a capacidade de storage de todo o grid

Monitore a capacidade de storage do seu grid para garantir que haja espaço livre suficiente 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 a adição de Storage Nodes ou volumes de storage antes que a capacidade de storage utilizável do grid seja consumida.

O painel do Grid Manager permite que você avalie rapidamente quanto espaço de storage está disponível para toda a grid e para cada data center. A página Nodes fornece valores mais detalhados para dados de

objetos e metadados de objetos.

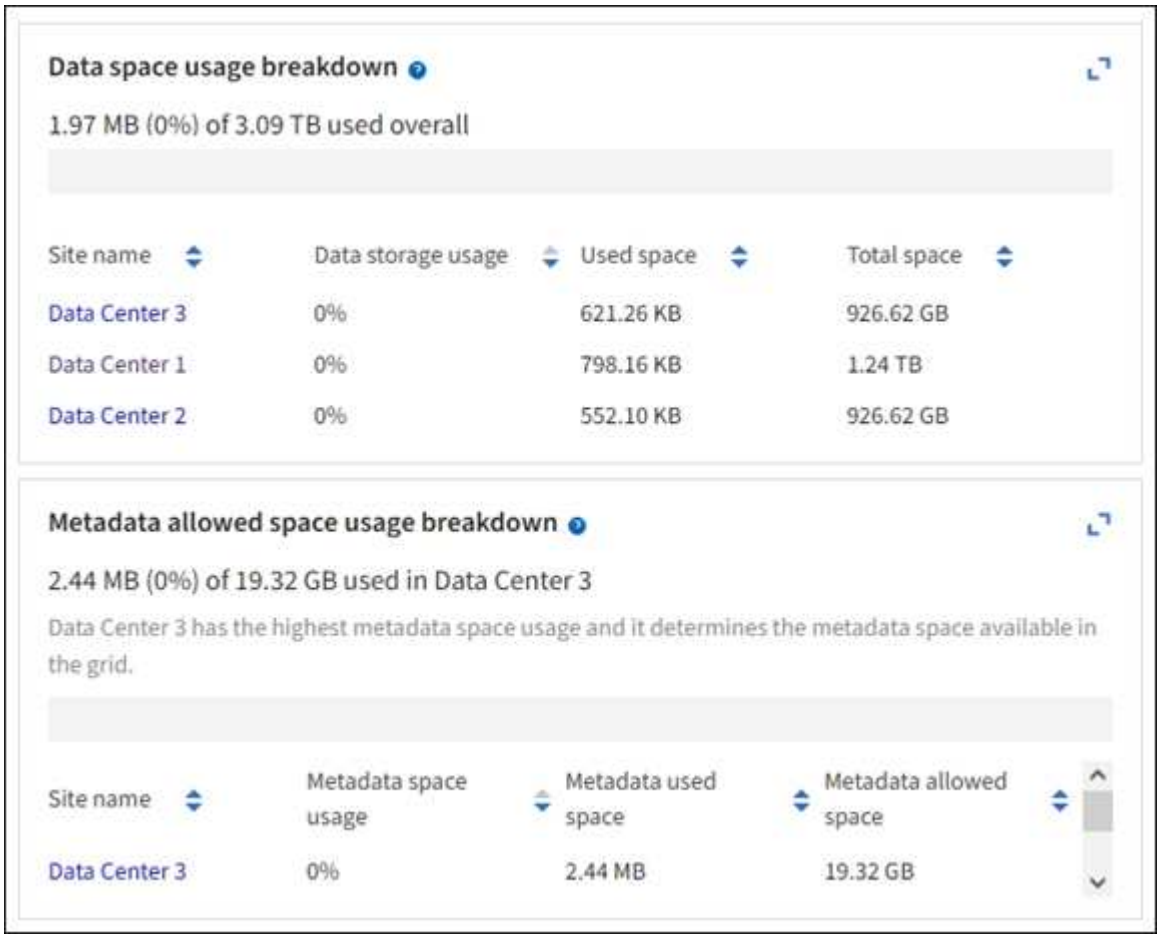
Passos

1. Avalie quanto espaço de storage está disponível para toda a grid e para cada data center.

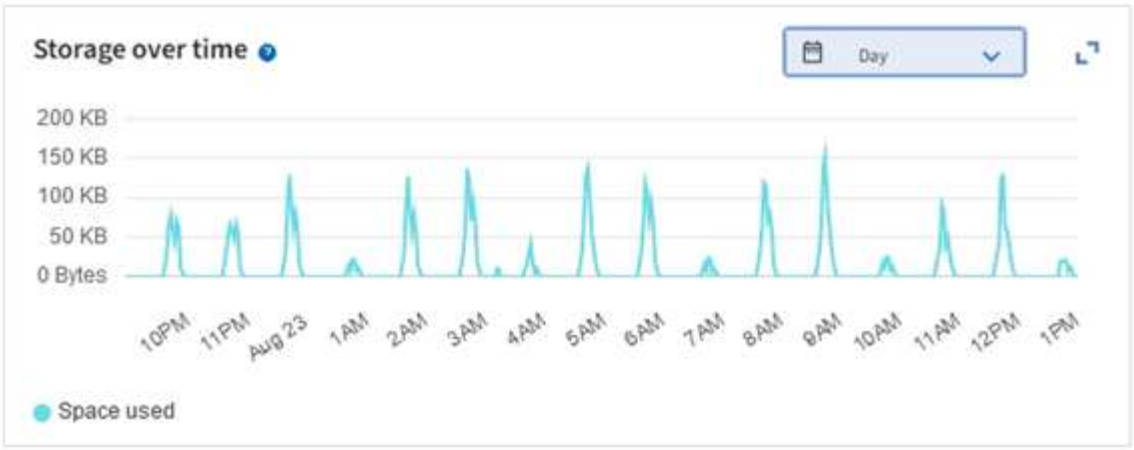
   a. Selecione **Dashboard > Visão geral**.

   b. Observe os valores nos cartões de detalhamento do uso do espaço de dados e de detalhamento do uso do espaço permitido para metadados. Cada cartão lista uma porcentagem de uso do storage, a capacidade do espaço utilizado e o espaço total disponível ou permitido por site.

   O resumo não inclui mídias de arquivamento.



   a. Observe o gráfico no cartão "Storage over time". Use o menu suspenso de período para ajudar você a determinar a rapidez com que o storage é consumido.



2. Use a página Nós para obter detalhes adicionais sobre quanto espaço de storage foi usado e quanto espaço de storage ainda está disponível na grid para dados de objeto e metadados de objeto.
   a. Selecione **Nós**.
   b. Selecione ***grid*** > **Storage**.

   c. Posicione o cursor sobre os gráficos **Storage used - object data** e **Storage used - object metadata** para ver quanto storage de objetos e quanto storage de metadados de objetos está disponível para toda a grid, e quanto foi usado ao longo do tempo.

> Os valores totais para um site ou para a grid não incluem nós que não reportaram métricas por pelo menos cinco minutos, como nós offline.

3. Planeje realizar uma expansão para adicionar nós de armazenamento ou volumes de armazenamento antes que a capacidade de storage do grid seja consumida.

   Ao planejar o cronograma de uma expansão, leve em consideração quanto tempo levará para adquirir e instalar storage adicional.

Se a sua política ILM utiliza codificação de apagamento, você pode preferir expandir quando os nós de Storage existentes estiverem aproximadamente 70% cheios, para reduzir o número de nós que precisam ser adicionados.

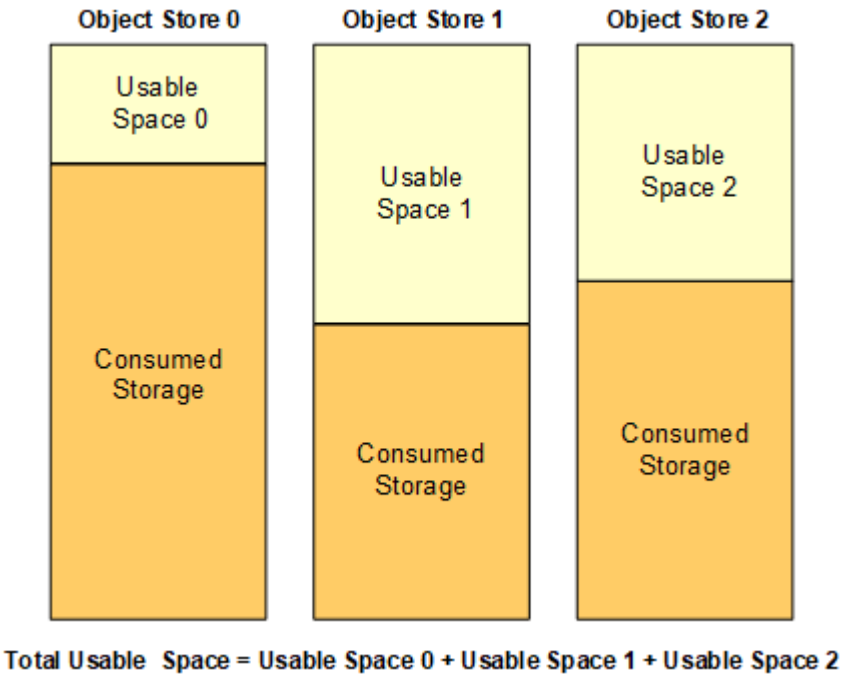
Para obter mais informações sobre o planejamento de uma expansão de storage, consulte o "instruções para expandir StorageGRID".

Monitore a capacidade de storage de cada Storage Node

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

Sobre esta tarefa

O espaço utilizável é a quantidade de espaço de storage disponível para armazenar objetos. O espaço utilizável total de um Storage Node é calculado somando o espaço disponível em todos os storages de objetos dentro do nó.



Passos

1. Selecione **Nodes** > ***Storage Node*** > **Storage**.

   Os gráficos e tabelas do nó são exibidos.

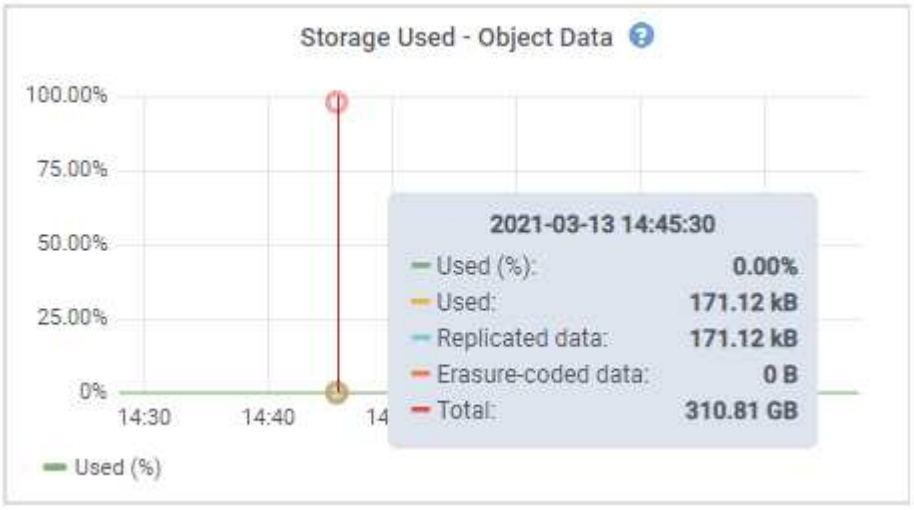
2. Posicione o cursor sobre o gráfico "Storage used - object data".

   Os seguintes valores são exibidos:

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

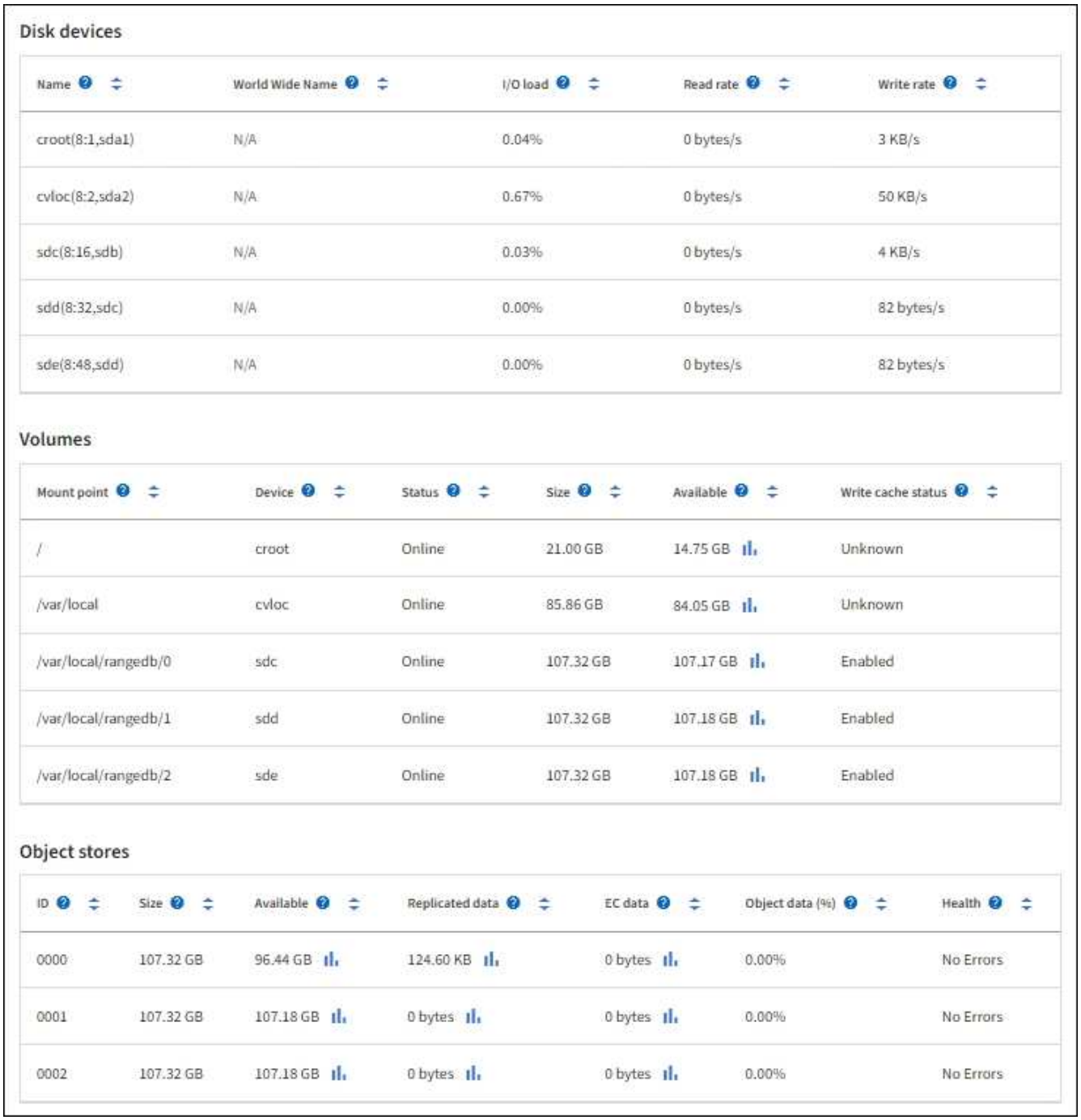
por apagamento neste nó, site ou grid.

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



3. Analise os valores disponíveis nas tabelas de volumes e object stores, abaixo dos gráficos.

Para visualizar gráficos desses 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 em que o espaço de storage utilizável está sendo consumido.
5. Para manter o funcionamento normal do sistema, adicione Storage Nodes, adicione volumes de armazenamento ou arquive dados de objetos antes que o espaço utilizável seja consumido.

   Ao planejar o cronograma de uma expansão, leve em consideração quanto tempo levará para adquirir e instalar storage adicional.

   > Se a sua política ILM utiliza codificação de apagamento, você pode preferir 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 o planejamento de uma expansão de storage, consulte o "instruções

para expandir StorageGRID".

O "Baixo storage de objetos" alerta é acionado quando não há espaço suficiente para armazenar dados de objetos em um Storage Node.

Monitore a capacidade de metadados de objetos para cada Storage Node

Monitore o uso de metadados para cada Storage Node para garantir que haja espaço suficiente disponível para as operações essenciais do banco de dados. Você deve adicionar novos Storage Nodes em cada site antes que os metadados de objetos excedam 100% do espaço de metadados permitido.

Sobre esta tarefa

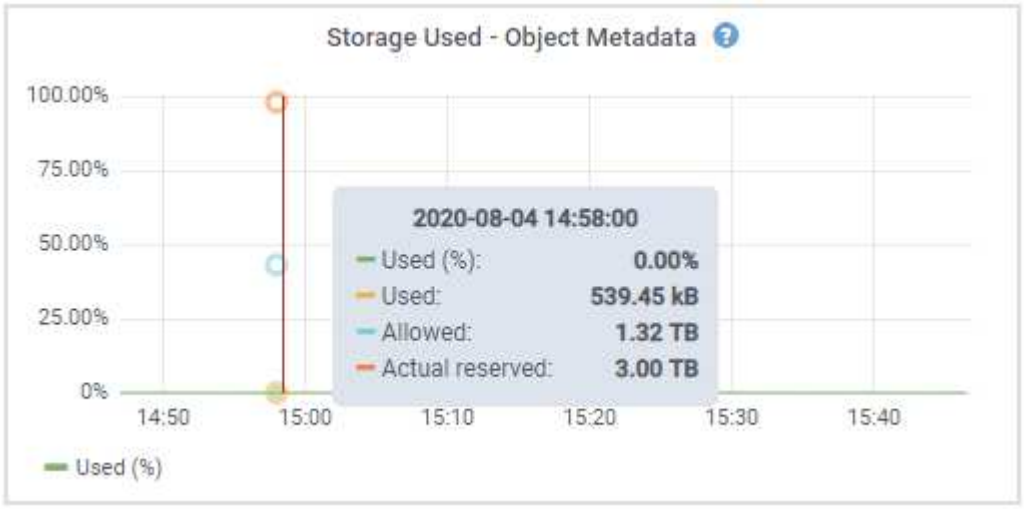
StorageGRID mantém três cópias dos metadados de objetos em cada site para fornecer redundância e proteger os metadados de objetos contra perda. As três cópias são distribuídas uniformemente entre todos os Storage Nodes em cada site, utilizando o espaço reservado para metadados no volume de storage 0 de cada Storage Node.

Em alguns casos, a capacidade de metadados de objetos da grid pode ser consumida mais rapidamente do que a capacidade de storage de objetos. Por exemplo, se você normalmente ingere grandes quantidades de objetos pequenos, pode ser necessário adicionar Storage Nodes para aumentar a capacidade de metadados, mesmo que ainda 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 partes em um upload multipart e a frequência de alterações nos locais de storage do ILM.

Passos

1. Selecione **Nodes** > ***Storage Node*** > **Storage**.
2. Posicione o cursor sobre o gráfico "Storage used - object metadata" para ver os valores de um horário específico.



Usado (%)

A porcentagem do espaço de metadados permitido que foi utilizada neste Storage Node.

Métricas do Prometheus: `storagegrid_storage_utilization_metadata_bytes` e `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

Os bytes do espaço de metadados permitido que foram usados neste Storage Node.

Métrica do Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

O espaço reservado para metadados neste Storage Node. Para saber como esse valor é determinado para cada Storage Node, consulte o "Descrição completa do espaço de metadados permitido".

Métrica do Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Espaço reservado real

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

A métrica Prometheus será adicionada em uma versão futura.

> Os valores totais para um site ou para a grid não incluem nós que não reportaram métricas por pelo menos cinco minutos, como nós offline.

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

> O alerta **Armazenamento de metadados insuficiente** é acionado quando o valor de **Usado (%)** atinge determinados limites. Resultados indesejáveis podem ocorrer se os metadados de objetos utilizarem mais de 100% do espaço permitido.

Ao adicionar novos nós, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de armazenamento do site. Consulte o "Instruções para expandir um sistema StorageGRID".

Monitorar previsões de uso do espaço

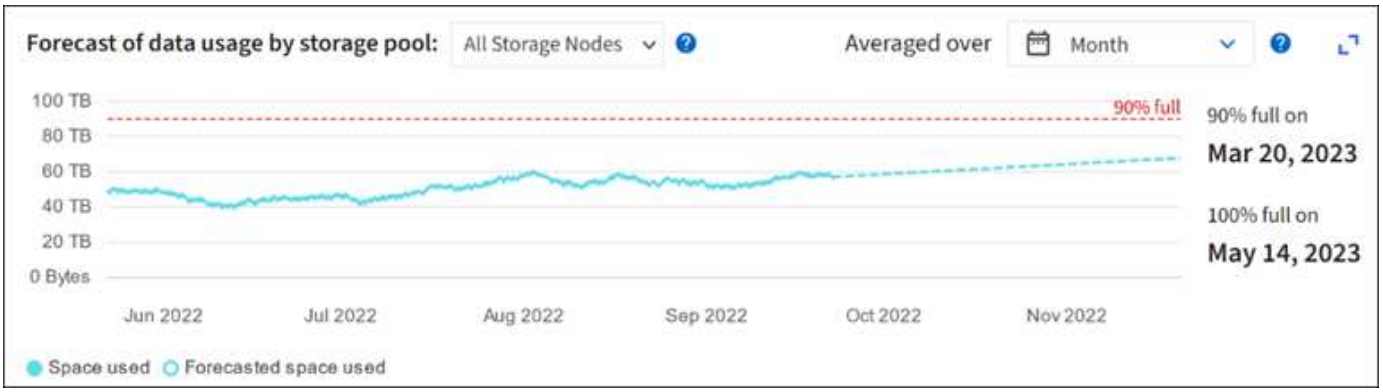
Monitore as previsões de uso de espaço para dados de usuário e metadados para estimar quando você precisará "expandir uma grid".

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

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

Passos

1. No painel, selecione **Storage**.
2. Visualize os cartões do painel de controle, a previsão de uso de dados por pool de storage e a previsão de uso de metadados por site.
3. Use esses valores para estimar quando você precisará adicionar novos Storage Nodes para armazenamento de dados e metadados.



Monitore o gerenciamento do ciclo de vida das informações no StorageGRID

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

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 criadas, onde as cópias são armazenadas e o tempo durante o qual cada cópia é retida.

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

Use a guia do painel do Grid Manager

Passos

Utilize a aba ILM no painel do Grid Manager para monitorar as operações de ILM:

1. Faça login no Grid Manager.
2. No painel de controle, selecione a guia ILM e anote os valores no cartão da fila ILM (Objects) e no cartão da taxa de avaliação ILM.

   Picos temporários na fila ILM (Objetos) no painel de controle são esperados. Mas se a fila continuar aumentando e nunca diminuir, a grid precisa de mais recursos para operar com eficiência: seja mais Storage Nodes ou, se a política ILM alocar objetos em locais remotos, mais largura de banda.

Use a página Nodes

Passos

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

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

1. Selecione **Nós**.

2. Selecione ***grid name*** > **ILM**.
3. Posicione o cursor sobre o gráfico da fila ILM para visualizar o valor dos seguintes atributos em um determinado momento:
   - **Objetos enfileirados (de operações do cliente)**: o número total de objetos aguardando avaliação do gerenciamento do ciclo de vida das informações devido a operações do cliente (por exemplo, ingest).
   - **Objetos enfileirados (de todas as operações)**: o número total de objetos aguardando avaliação do ILM.
   - **Taxa de varredura (objetos/seg)**: a taxa na qual os objetos na grid são varridos e enfileirados para ILM.
   - **Taxa de avaliação (objetos/seg)**: a taxa atual na qual os objetos estão sendo avaliados em relação à política ILM no grid.

   > A seção de fila ILM está incluída apenas para a grid. Essas informações não são exibidas na guia ILM de um site ou Storage Node.

4. Na seção Fila ILM, observe os seguintes atributos.
   - **Período de digitalização - estimado**: tempo estimado para concluir uma digitalização completa do ILM de todos os objetos.

     > Uma varredura completa não garante que o gerenciamento do ciclo de vida das informações (ILM) tenha sido aplicado a todos os objetos.

   - **Tentativas de reparo**: O número total de operações de reparo de objetos para dados replicados que foram tentadas. Essa contagem incrementa cada vez que um Storage Node tenta reparar um objeto de alto risco. Os reparos de ILM de alto risco são priorizados se a grid ficar ocupada.

     O reparo do mesmo objeto pode incrementar novamente se a replicação falhar após o reparo. Esses atributos podem ser úteis quando você estiver monitorando o progresso da recuperação do volume do Storage Node. Se o número de reparos tentados parar de aumentar e uma verificação completa for concluída, o reparo provavelmente foi concluído.

5. Alternativamente, envie uma consulta Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` e `storagegrid_ilm_repairs_attempted`.

Monitore os recursos de rede e do sistema no StorageGRID

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

Monitore as conexões de rede e o desempenho

A conectividade de rede e a largura de banda são especialmente importantes se sua política de gerenciamento do ciclo de vida das informações (ILM) copiar objetos replicados entre sites ou armazenar objetos com código de apagamento usando um esquema que ofereça proteção contra perda de site. Se a rede entre os sites não estiver disponível, a latência de rede for muito alta ou a largura de banda for insuficiente, algumas regras de ILM podem não conseguir colocar os objetos onde esperado. Isso pode levar a falhas de ingestão (quando a opção de ingestão estrita estiver selecionada para as regras de ILM), ou a um desempenho de ingestão ruim e acúmulo de tarefas no ILM.

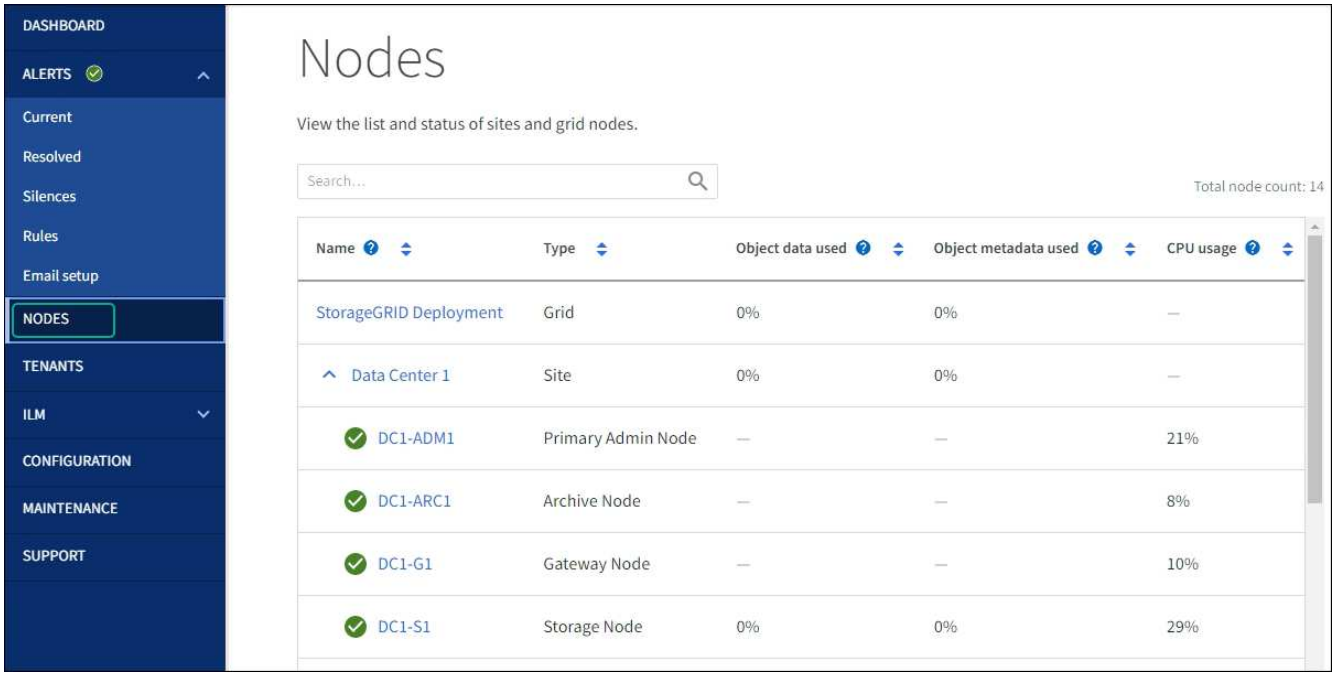
Utilize o Grid Manager para monitorar a conectividade e o desempenho da rede, para que você possa resolver quaisquer problemas prontamente.

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

Passos

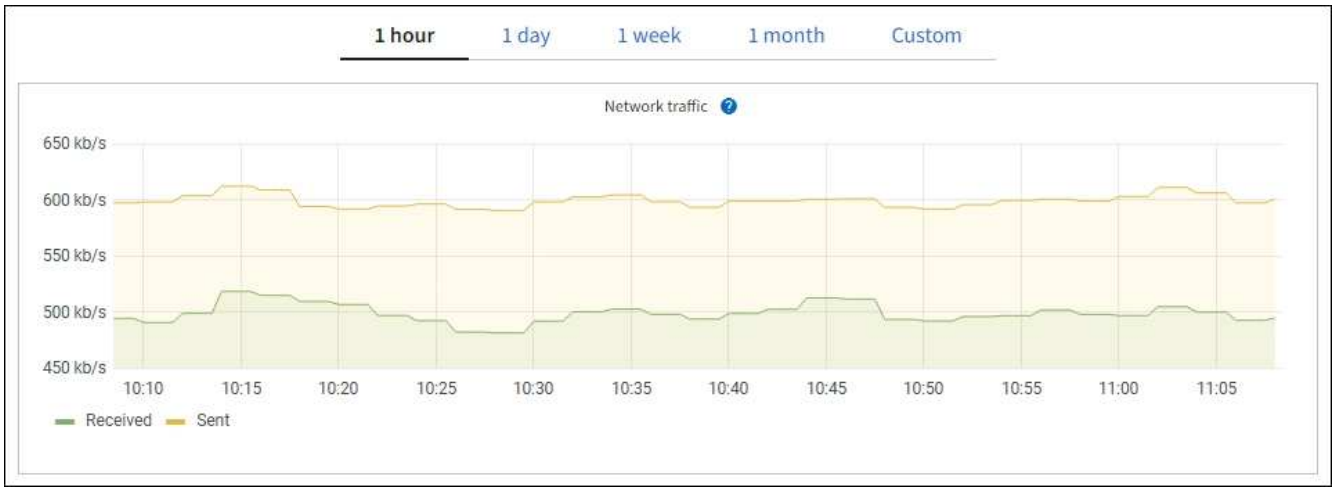
1. Selecione **Nós**.

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



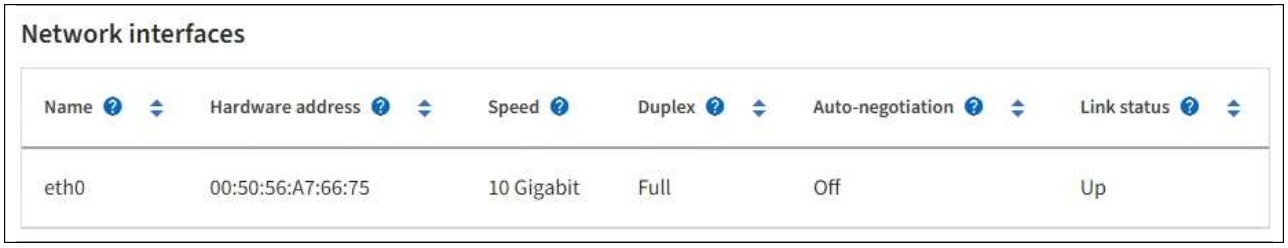
2. Selecione o nome da grid, um site de data center específico ou um nó da grid e, em seguida, selecione a guia **Rede**.

   O gráfico de tráfego de rede fornece um resumo do tráfego de rede para o grid como um todo, para o data center ou para o nó.



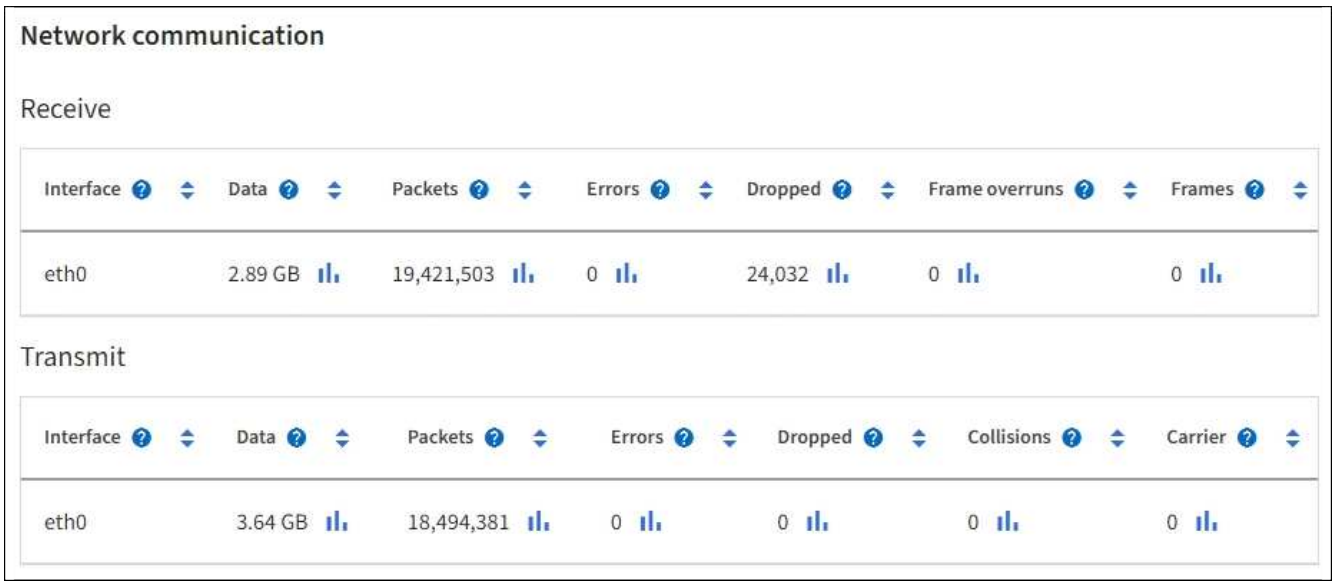
   a. Se você selecionou um nó da grade, role para baixo para revisar a seção **Interfaces de rede** da

página.



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

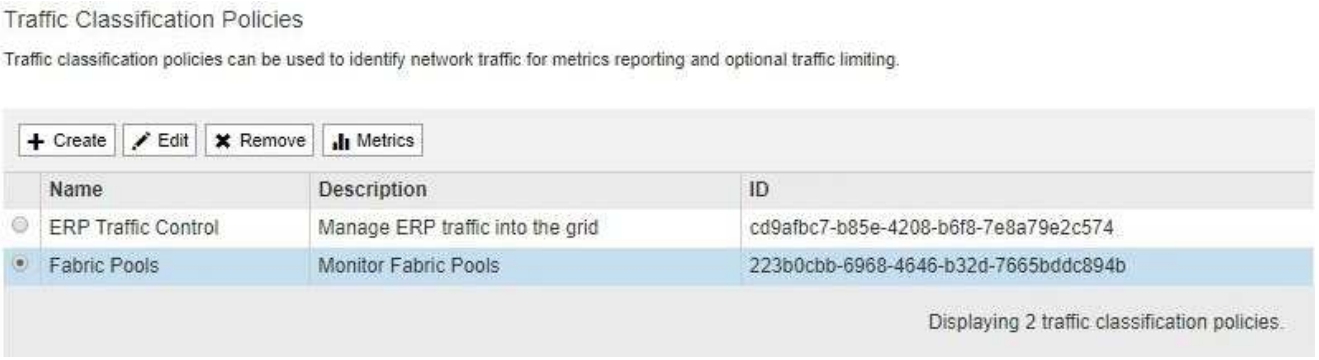
   As tabelas de Recebimento e Transmissão mostram quantos bytes e pacotes foram recebidos e enviados em cada rede, bem como outras métricas de recebimento e transmissão.



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

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

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



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

b. Analise 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 com que frequência o tráfego é limitado e decida se a política continua atendendo às suas necessidades. De tempos em tempos, "Ajuste cada política de classificação de tráfego conforme necessário".

Informações relacionadas

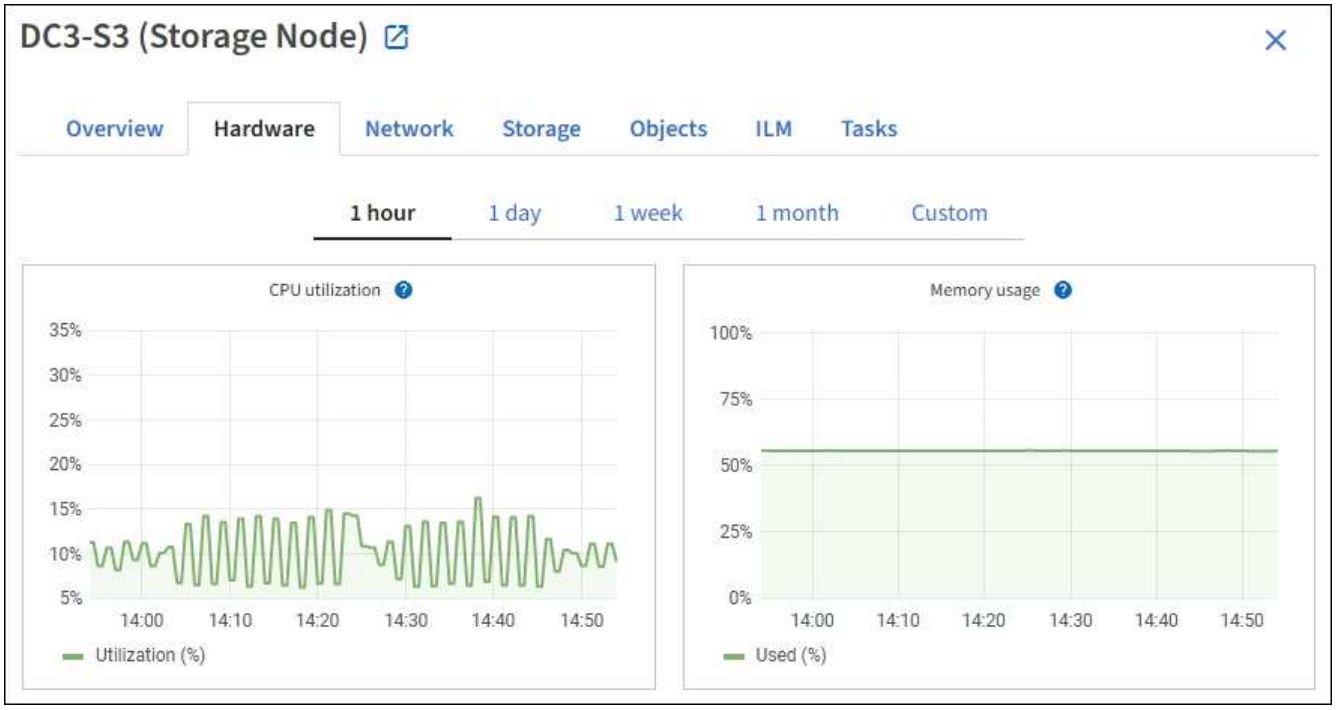
- "Veja a aba Rede"
- "Monitorar os estados de conexão dos nós"

Monitorar recursos em nível de nó

Monitore os nós individuais da grid para verificar seus níveis de uso de recursos. Se os nós estiverem constantemente sobrecarregados, pode ser necessário adicionar mais nós para operações eficientes.

Passos

1. Na página **Nós**, selecione o nó.
2. Selecione a aba **Hardware** para exibir os gráficos de utilização da CPU e uso de memória.



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

Informações relacionadas

- "Veja informações sobre Storage Nodes de dispositivos"
- "Veja informações sobre os nós de administração e os nós de gateway do appliance"

Monitore a atividade do tenant no StorageGRID

Toda a atividade do cliente S3 está associada às contas de locatário do StorageGRID. Você pode usar o Grid Manager para monitorar o uso de storage ou o tráfego de rede de todos os locatários ou de um locatário específico. Você pode usar o log de auditoria ou os painéis do Grafana para coletar informações mais detalhadas sobre como os locatários estão usando StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Acesso à raiz ou permissão para contas de locatário".

Ver todos os tenants

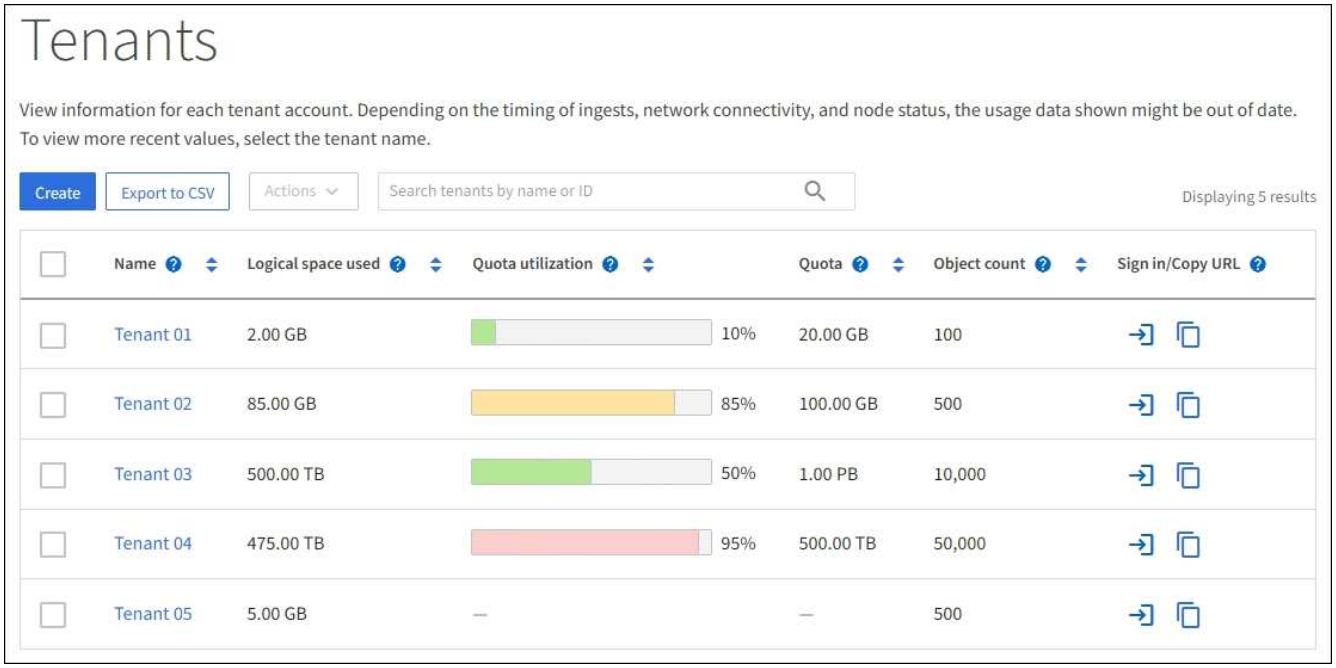
A página de Tenants exibe informações básicas para todas as contas de tenants atuais.

Passos

1. Selecione **Tenants**.
2. Analise as informações apresentadas nas páginas do tenant.

   O espaço lógico utilizado, a utilização da quota, a quota e a contagem de objetos são listados para cada locatário. Se uma quota não estiver definida para um locatário, os campos utilização da quota e quota conterão um traço (—).

   > O tamanho lógico de todos os objetos pertencentes a este locatário inclui uploads multipartes incompletos e em andamento. O tamanho não inclui espaço físico adicional usado para políticas de ILM. Os valores de espaço usado são estimativas. Essas estimativas são afetadas pelo momento das ingestões, conectividade de rede e status do nó.



3. Opcionalmente, faça login em uma conta de locatário selecionando o link de login na coluna **Entrar/Copiar URL**.

4. Opcionalmente, copie a URL da página de login de um locatário selecionando o link na coluna "Entrar/Copiar URL".
5. Opcionalmente, selecione **Exportar para CSV** para visualizar e exportar um arquivo `.csv` contendo os valores de uso de todos os locatários.

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

   O conteúdo do arquivo `.csv` é semelhante ao 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 arquivo `.csv` 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 locatários. Consulte "Excluir conta de locatário".

   Você não pode remover uma conta de locatário se a conta incluir qualquer bucket ou contêiner.

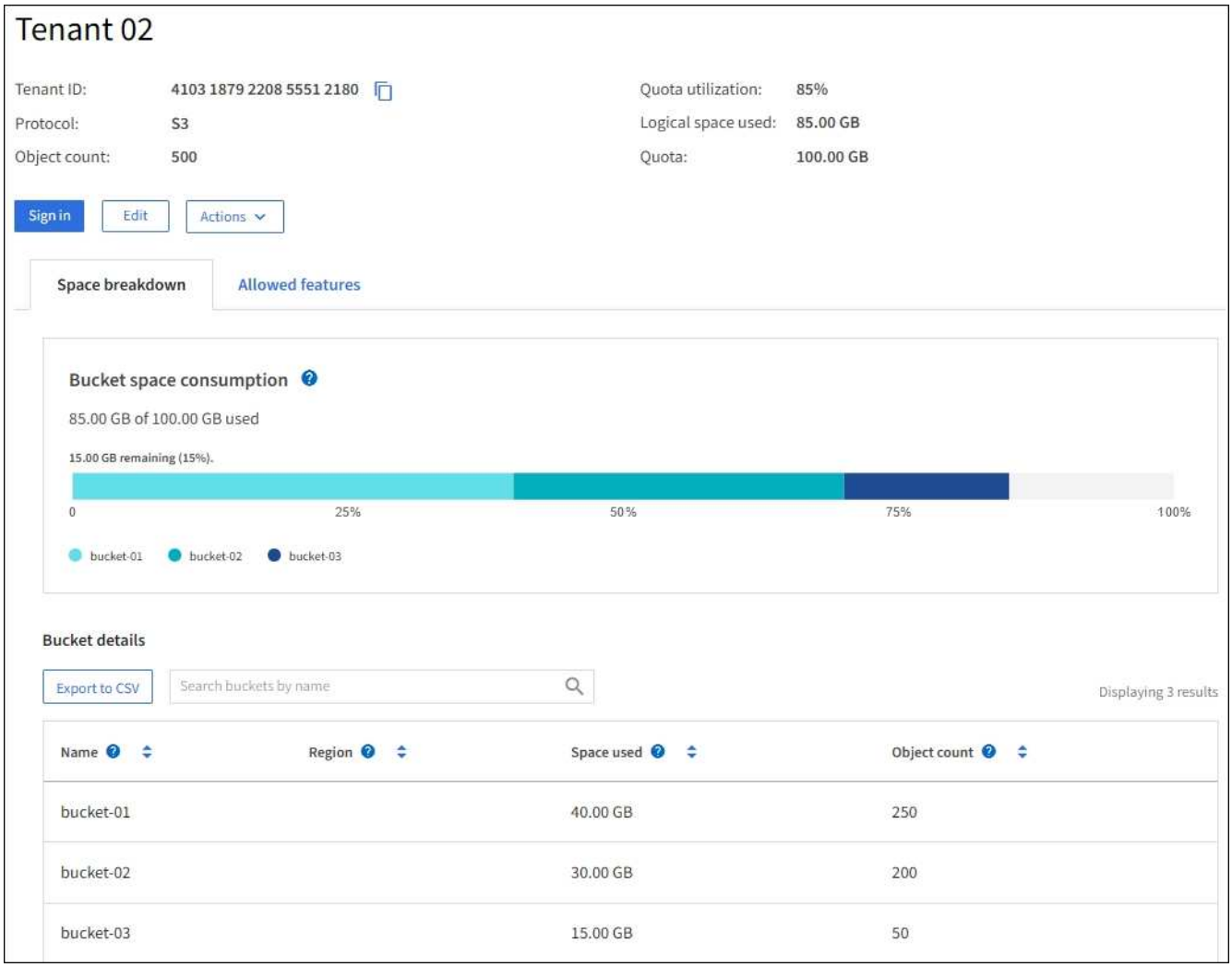
Veja um tenant específico

Você pode visualizar os detalhes de um tenant específico.

Passos

1. Selecione o nome do tenant na página Tenants.

   A página de detalhes do tenant é exibida.



2. Consulte a visão geral do tenant no topo da página.

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

   > O tamanho lógico de todos os objetos pertencentes a este locatário inclui uploads multipartes incompletos e em andamento. O tamanho não inclui espaço físico adicional usado para políticas de ILM. Os valores de espaço usado são estimativas. Essas estimativas são afetadas pelo momento das ingestões, conectividade de rede e status do nó.

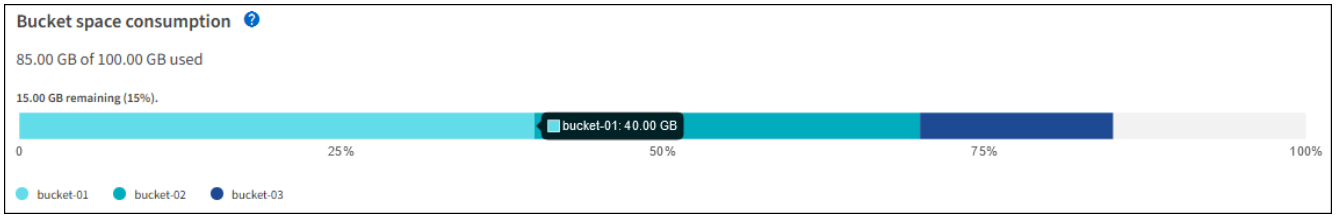
3. Na aba **Distribuição de espaço**, revise o gráfico de **Consumo de espaço**.

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

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

   Você pode posicionar o cursor sobre o gráfico de barras para visualizar o storage utilizado por cada bucket ou contêiner. Você pode posicionar o cursor sobre o segmento de espaço livre para ver a quantidade de

quota de storage restante.



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

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

Você pode ativar a regra de alerta **Uso excessivo da cota do locatário** para determinar se os locatários estão consumindo suas cotas. Se ativada, esse alerta é acionado quando um locatário atinge 90% de sua cota. Para obter instruções, consulte "Editar regras de alerta".

4. Na aba **Space breakdown**, revise os **Bucket details**.

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

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

   O conteúdo de um arquivo `.csv`de um locatário S3 individual 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 arquivo `.csv` 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 habilitados para o tenant. Veja "Editar conta de tenant" se você precisar alterar alguma dessas configurações.
7. Se o locatário tiver a permissão **Usar conexão de federação de grid**, opcionalmente selecione a guia **Federação de grid** para saber mais sobre a conexão.

   Veja "O que é federação de grid?" e "Gerenciar os inquilinos permitidos para a federação de grid".

Visualizar tráfego de rede

Se existirem políticas de classificação de tráfego para um tenant, analise o tráfego de rede desse tenant.

Passos

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

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

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

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

Utilize o log de auditoria

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

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

- Operações específicas do cliente, como PUT, GET ou DELETE
- Tamanhos de objetos
- A regra ILM aplicada a objetos
- O endereço 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 de sua preferência. Isso permite que você entenda melhor as atividades do cliente ou implemente modelos sofisticados de chargeback e cobrança.

Consulte "Analisar registros de auditoria" para mais informações.

Usar métricas Prometheus

Opcionalmente, utilize métricas do Prometheus para gerar relatórios sobre a atividade dos tenants.

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

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

- Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **API documentation**. Você pode usar as métricas na seção Metrics da Grid Management API para criar regras de alerta e painéis personalizados para a atividade do tenant.

Consulte "Análise das métricas de suporte" para mais informações.

Monitore as operações do cliente S3 no StorageGRID

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

Antes de começar

Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

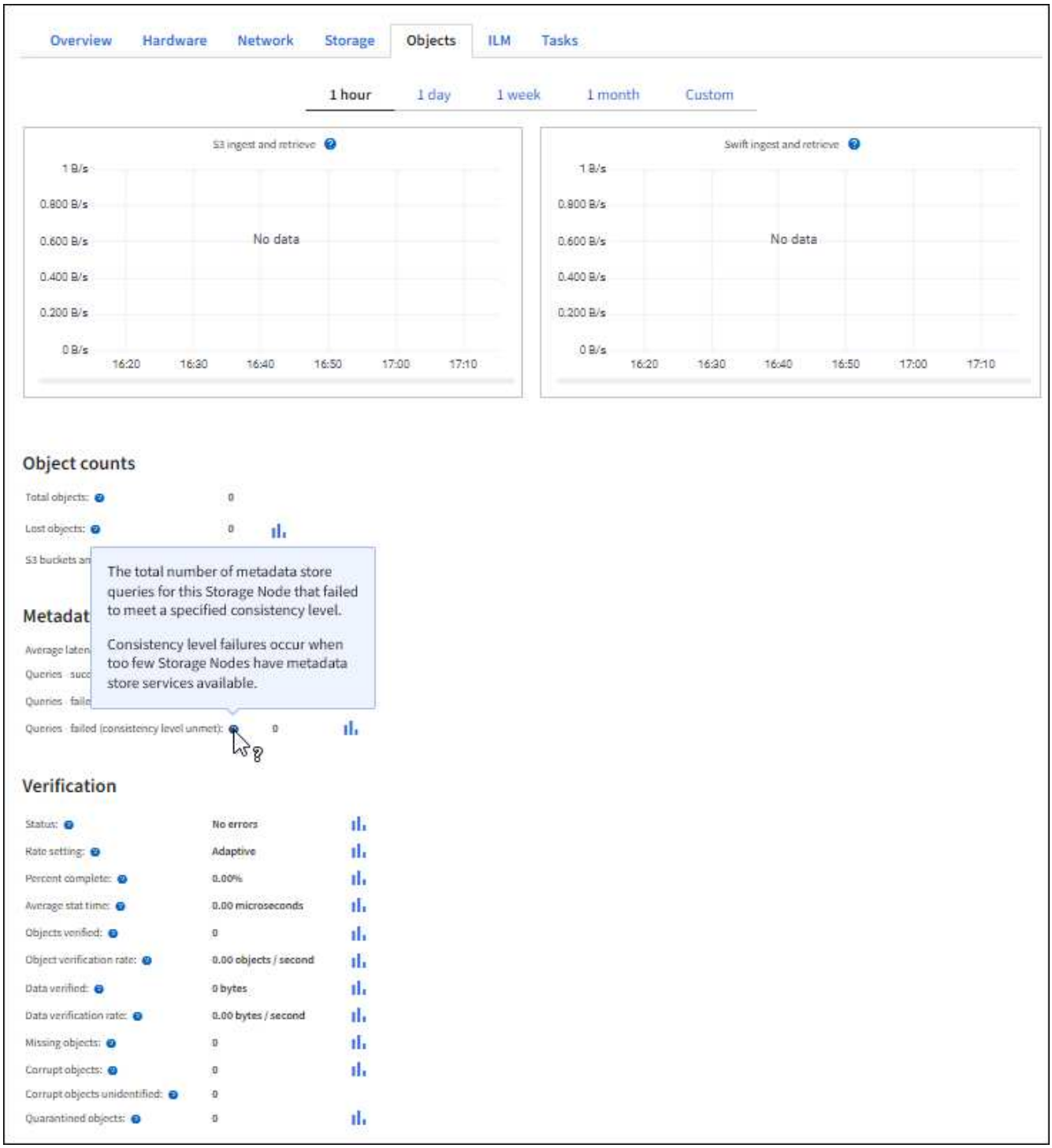
Passos

1. No dashboard, selecione a guia **Desempenho**.
2. Consulte os gráficos do S3, que resumem o número de operações de clientes realizadas pelos nós de armazenamento e o número de solicitações de API recebidas pelos nós de armazenamento durante o período selecionado.
3. Selecione **Nodes** para acessar a página de Nodes.
4. Na página inicial de Nodes (nível da grid), selecione a guia **Objects**.

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

5. Para visualizar informações sobre um Storage Node específico, selecione o nó na lista à esquerda e selecione a guia **Objetos**.

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



Monitore as operações de balanceamento de carga no StorageGRID

Se você estiver usando um balanceador de carga para gerenciar as conexões de clientes com o StorageGRID, deve monitorar as operações de balanceamento de carga após configurar o sistema inicialmente e após fazer quaisquer alterações de configuração ou realizar uma expansão.

Sobre esta tarefa

Você pode usar o serviço Load Balancer em Nós de Administração, Nós de Gateway ou um balanceador de carga externo de terceiro para distribuir as solicitações do cliente entre vários Nós de Armazenamento.

Após configurar o balanceamento de carga, você deve confirmar se as operações de ingestão e recuperação de objetos estão sendo distribuídas uniformemente entre os Storage Nodes. A distribuição uniforme das solicitações garante que o StorageGRID permaneça responsivo às solicitações do cliente sob carga e pode ajudar a manter o desempenho do cliente.

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

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

Passos

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

      Os nós com a função de Primary e os nós que não fazem parte de um grupo de HA devem estar distribuindo ativamente as solicitações aos clientes.

   d. Para cada nó que deve estar distribuindo ativamente as solicitações do cliente, selecione o "Aba Load Balancer".
   e. Analise o gráfico de tráfego de solicitações do balanceador de carga da última semana para garantir que o nó tenha distribuído solicitações ativamente.

      Em um grupo de alta disponibilidade (HA) ativo-backup, os nós podem assumir a função de backup ocasionalmente. Durante esse período, os nós não distribuem solicitações de clientes.

   f. Analise o gráfico da taxa de requisições de entrada do Load Balancer da última semana para revisar a taxa de transferência de objetos do nó.
   g. Repita estes passos para cada nó de administração ou nó de gateway no sistema StorageGRID.
   h. Opcionalmente, utilize as políticas de classificação de tráfego para visualizar uma análise mais detalhada do tráfego atendido pelo serviço Load Balancer.
2. Verifique se essas solicitações estão sendo distribuídas uniformemente para os Storage Nodes.
   a. Selecione ***Nó de armazenamento*** > **LDR** > **HTTP**.
   b. Analise o número de **Sessões de entrada atualmente estabelecidas**.
   c. Repita para cada Storage Node na grid.

      O número de sessões deve ser aproximadamente igual em todos os Storage Nodes.

Monitorar conexões de federação de grid do StorageGRID

Você pode monitorar informações básicas sobre todas as "conexões de federação de grid" conexões, informações detalhadas sobre uma conexão específica ou métricas do Prometheus sobre operações de replicação entre grids. Você pode monitorar uma conexão de qualquer um dos grids.

Antes de começar

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

Ver todas as conexões

A página de federação de grid exibe informações básicas sobre todas as conexões de federação de grid e sobre todas as contas de locatário que têm permissão para usar conexões de federação de grid.

Passos

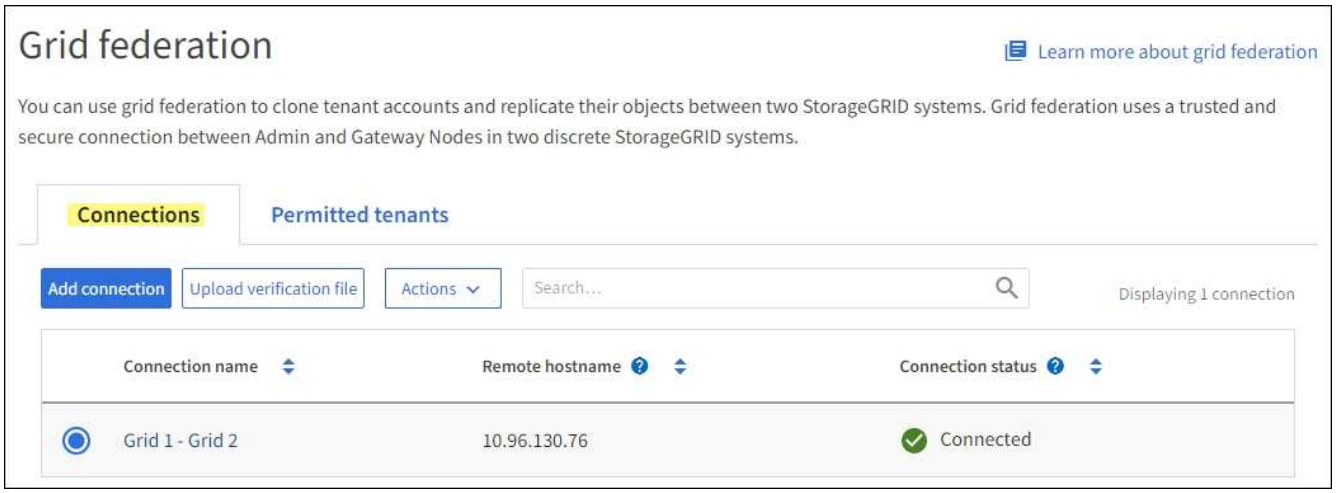
1. Selecione **Configuração** > **Sistema** > **Grid federation**.

   A página de federação Grid é exibida.

2. Para visualizar informações básicas sobre todas as conexões nesta grid, selecione a guia **Conexões**.

   Nesta aba, você pode:

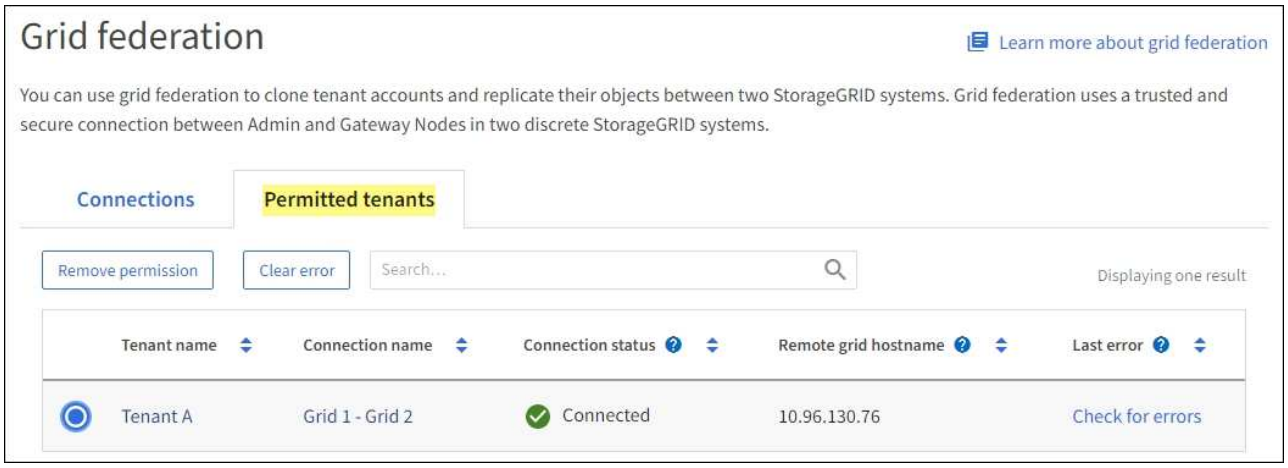
   - "Criar uma nova conexão".
   - Selecione uma conexão existente com "editar ou testar".



3. Para visualizar informações básicas de todas as contas de locatário nesta grid que possuem a permissão **Usar conexão de federação de grid**, selecione a guia **Locatários permitidos**.

   Nesta aba, você pode:

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



Ver uma conexão específica

Você pode visualizar os detalhes de uma conexão específica da federação de grid.

Passos

1. Selecione qualquer uma das abas na página de federação do Grid e, em seguida, selecione o nome da conexão na tabela.

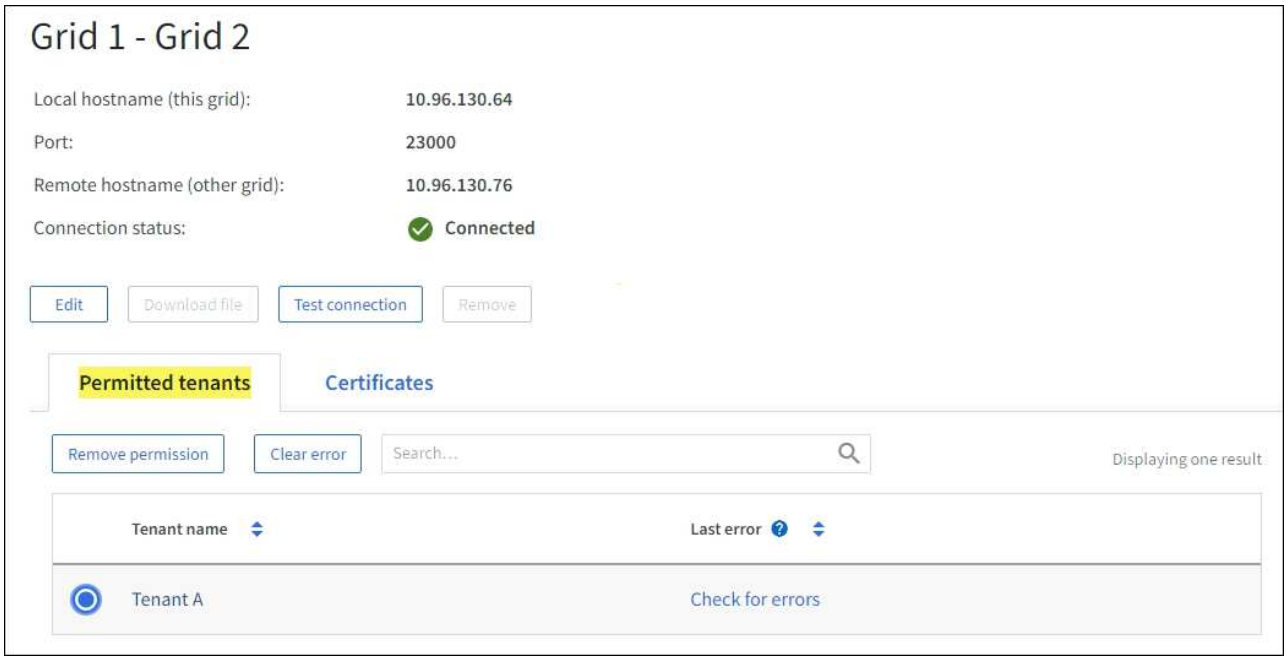
   Na página de detalhes da conexão, você pode:

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

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

   Nesta aba, você pode:

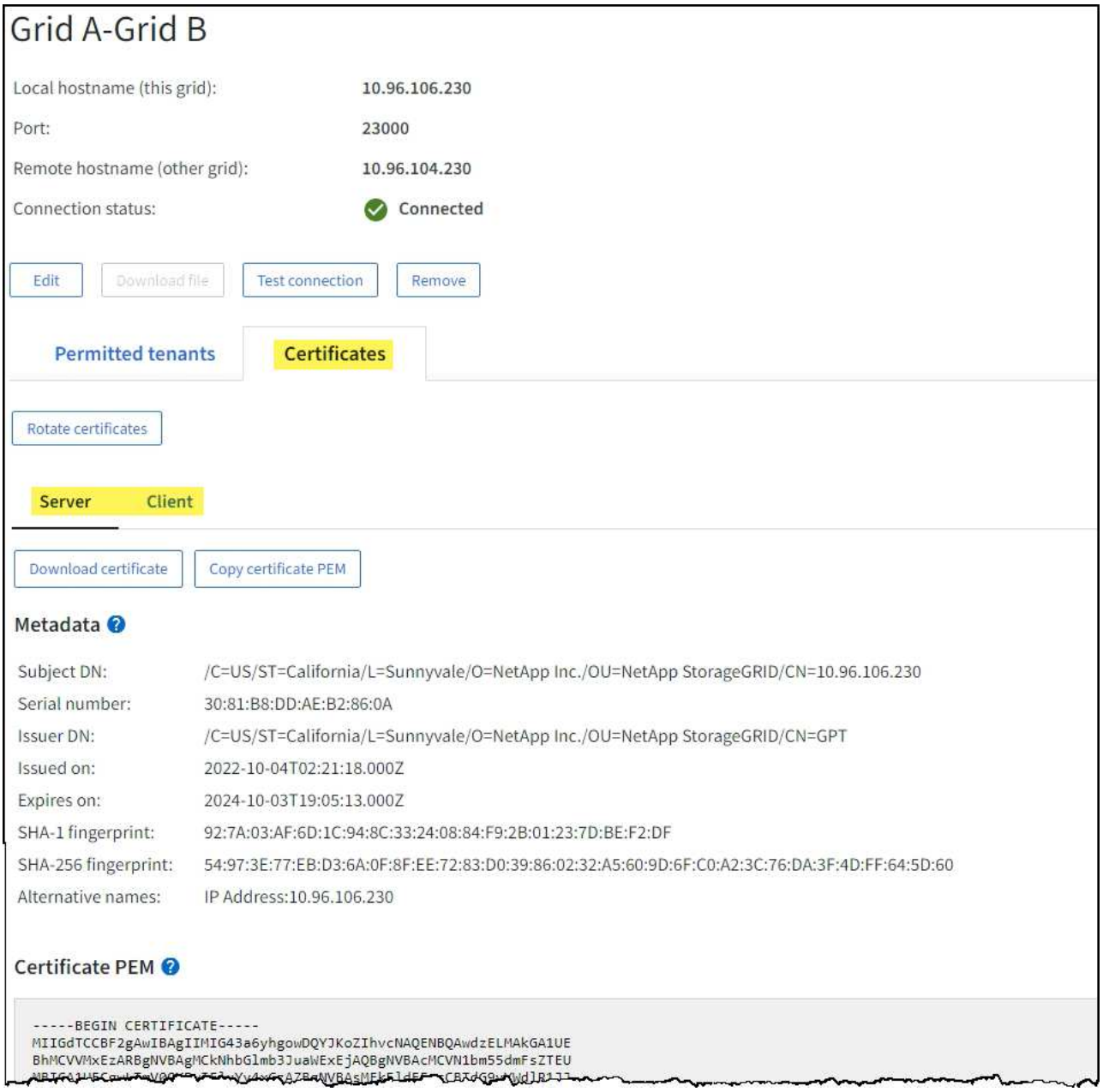
   - "Veja a página de detalhes de cada locatário permitido".
   - "Remover a permissão de um tenant" para usar a conexão.
   - Verifique se há erros de replicação entre grades e corrija o último erro. Consulte "Solucionar problemas de erros de federação de grid".



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

   Nesta aba, você pode:

   - "Rotacionar certificados de conexão".
   - Selecione **Server** ou **Client** para visualizar ou baixar o certificado associado ou copiar o certificado PEM.



Analisar métricas de replicação entre grids

Você pode usar o painel de controle Cross-Grid Replication no Grafana para visualizar as métricas do Prometheus sobre as operações de replicação entre grades em sua grade.

Passos

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

   As ferramentas disponíveis na página Métricas destinam-se ao uso pelo suporte técnico. Alguns recursos e itens de menu nessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Consulte a lista de "métricas Prometheus comumente usadas".

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

   Para obter instruções detalhadas, consulte "Análise das métricas de suporte".

3. Para tentar novamente a replicação de objetos que não foram replicados, consulte "Identifique e repita operações de replicação com falha".

Gerenciar alertas

Gerenciar alertas no StorageGRID

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

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

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

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

Para saber mais:

- Reveja os vídeos:

  Visão geral dos alertas

  Alertas personalizados

- Consulte o "Referência de alertas".

Visualizar regras de alerta do StorageGRID

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

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

Antes de começar

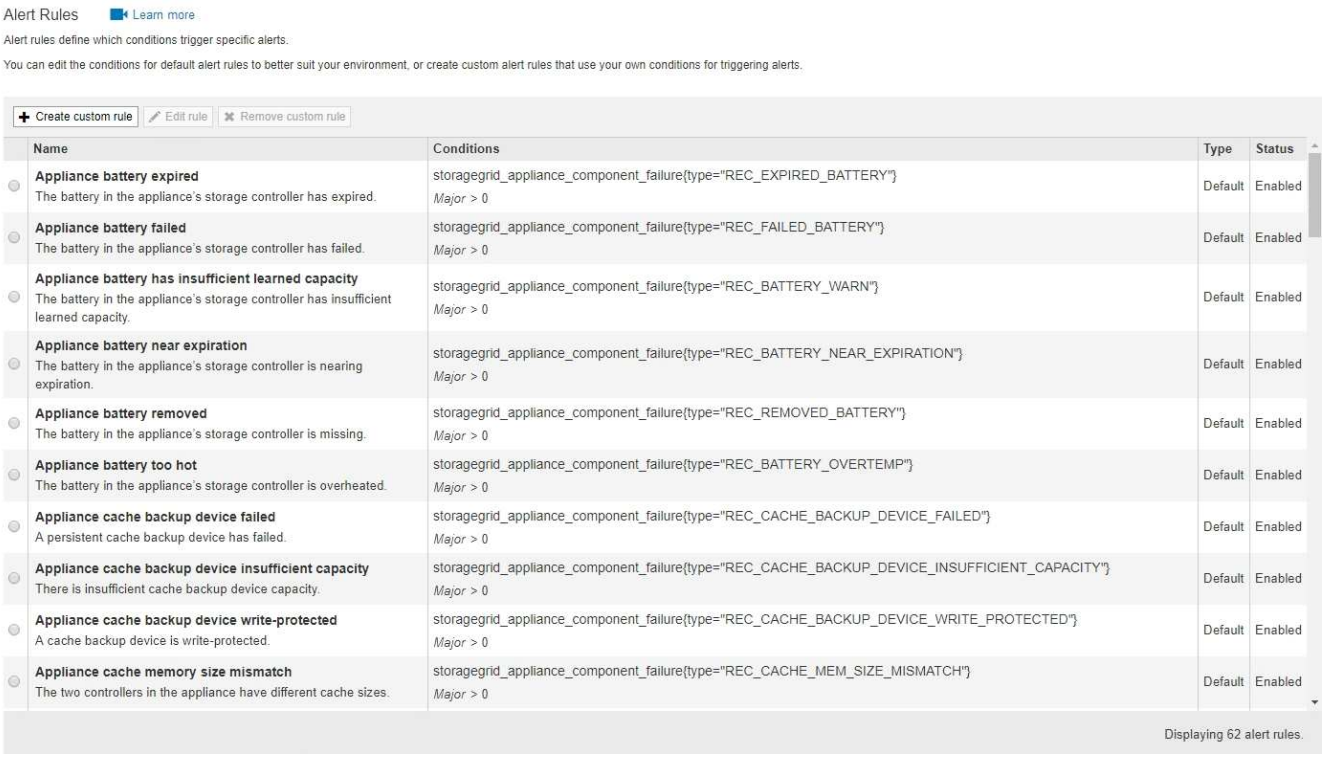
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Gerenciar alertas ou permissão de acesso root".
- Opcionalmente, você assistiu ao vídeo:

  Visão geral dos alertas

Passos

1. Selecione **Alertas** > **Regras**.

   A página Regras de Alerta é exibida.



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

Cabeçalho da coluna	Descrição
Nome	O nome e a descrição exclusivos 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.

Cabeçalho da coluna	Descrição
Condições	As expressões do Prometheus que determinam quando este alerta é acionado. Um alerta pode ser acionado em um ou mais dos seguintes níveis de gravidade, mas uma condição para cada gravidade não é obrigatória. • **Crítico**: Existe uma condição anormal que interrompeu o funcionamento normal de um nó ou serviço do StorageGRID. Você deve resolver o problema imediatamente. A não resolução do problema pode resultar em interrupção do serviço e perda de dados. • **Grave**: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar alertas graves e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um StorageGRID node ou serviço. • **Menor**: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se persistir. Você deve monitorar e resolver alertas menores que não se resolvem sozinhos para garantir que não resultem em um problema mais sério.
Tipo	O tipo de regra de alerta: • **Padrão**: Uma regra de alerta fornecida com o sistema. Você pode desativar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Você não pode remover uma regra de alerta padrão. • **Padrão***: Uma regra de alerta padrão que inclui uma condição ou duração editada. Se necessário, você pode facilmente reverter uma condição modificada para o padrão original. • **Personalizado**: Uma regra de alerta que você criou. Você pode desativar, editar e remover regras de alerta personalizadas.
Status	Indica 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 no StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Gerenciar alertas ou permissão de acesso root".
- Você está familiarizado com o "métricas Prometheus comumente usadas".

- Você entende o "sintaxe de consultas do Prometheus".
- Opcionalmente, você assistiu ao vídeo:

  Alertas personalizados

Sobre esta tarefa

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

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

  Por exemplo, para testar a expressão `node_memory_MemTotal_bytes < 24000000000`, primeiro execute `node_memory_MemTotal_bytes >= 0` e 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. A ausência de resultados 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.

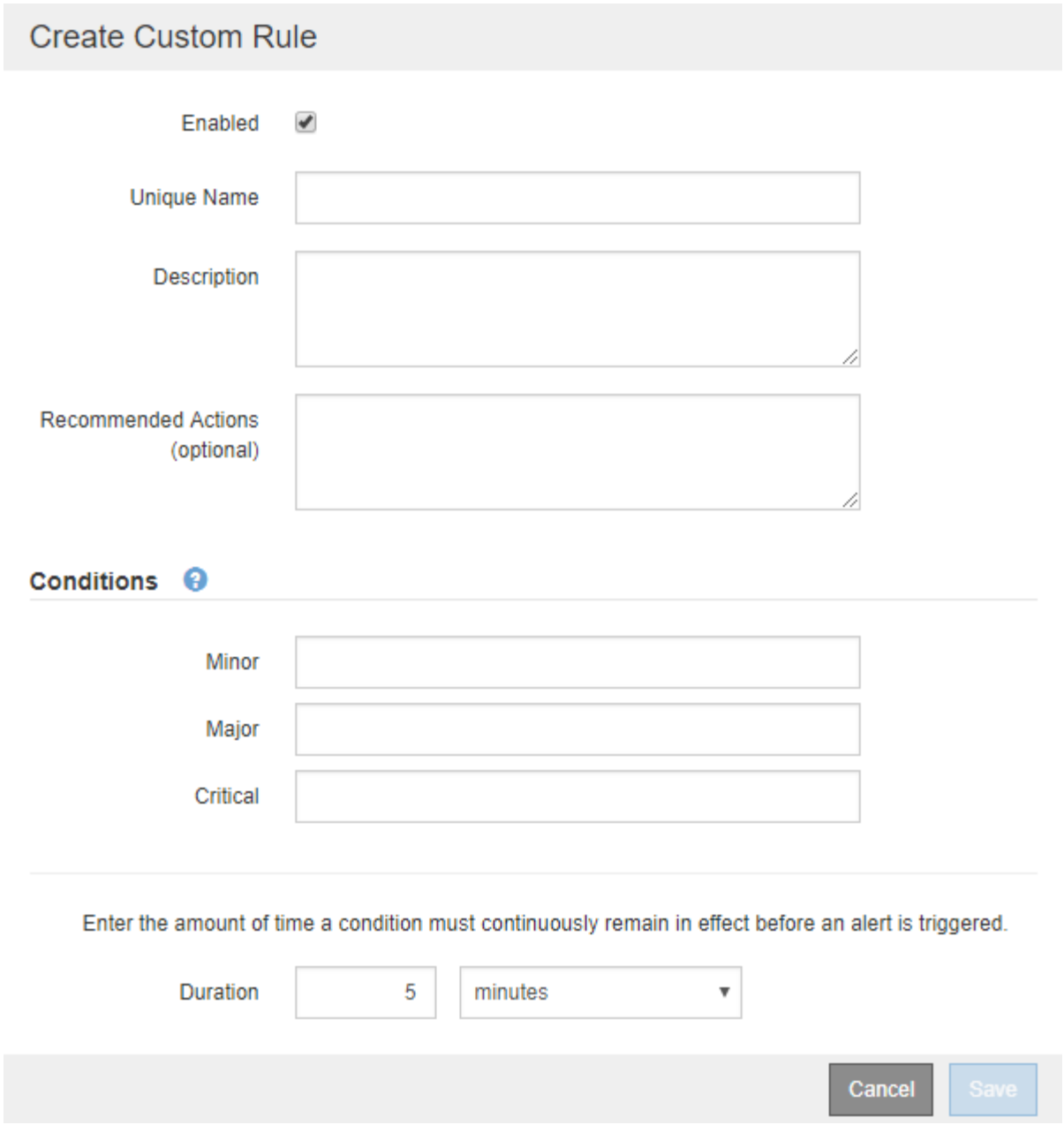
Passos

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. Selecione ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está atualmente habilitada.

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

4. Insira as seguintes informações:

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

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

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

   Uma expressão básica geralmente tem a seguinte forma:

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

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

   Essa expressão faz com que um alerta seja acionado se a quantidade de RAM instalada em um nó for inferior a 24.000.000.000 bytes (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Para visualizar métricas disponíveis e testar expressões do Prometheus, selecione o ícone de ajuda e siga o link para a seção Métricas da API de Gerenciamento de Grid.

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

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

   O padrão é 5 minutos.

7. Selecione **Salvar**.

   A caixa de diálogo fecha e a nova regra de alerta personalizada aparece na tabela de Alert Rules.

Editar regras de alerta no StorageGRID

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

Antes de começar

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

Sobre esta tarefa

Ao editar uma regra de alerta padrão, você pode alterar as condições para alertas 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 de acionamento, você pode não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

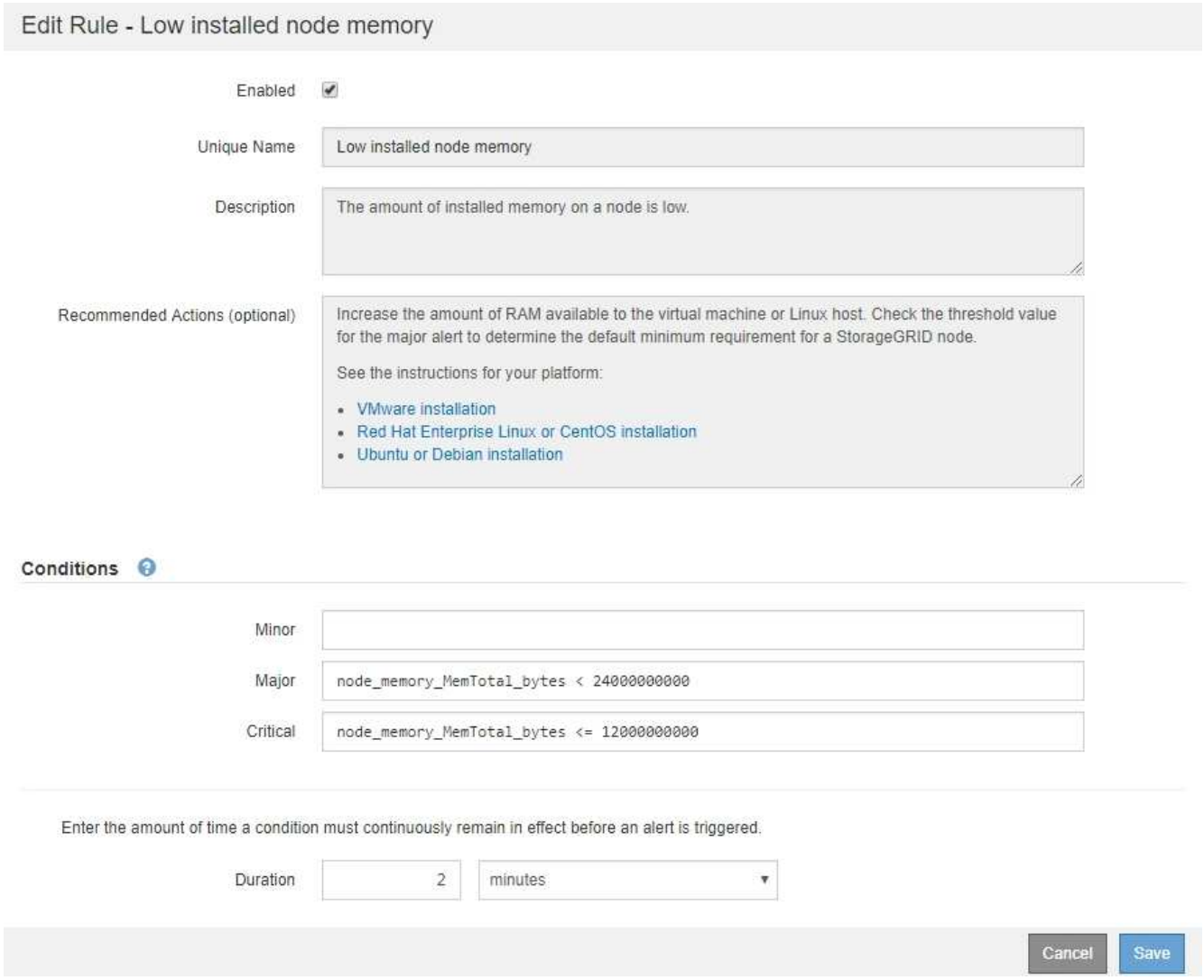
Passos

1. Selecione **Alertas** > **Regras**.

   A página Regras de Alerta é exibida.

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

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



4. Selecione ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está atualmente habilitada.

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

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

Em geral, desativar uma regra de alerta padrão não é recomendável. Se uma regra de alerta estiver desativada, você pode não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

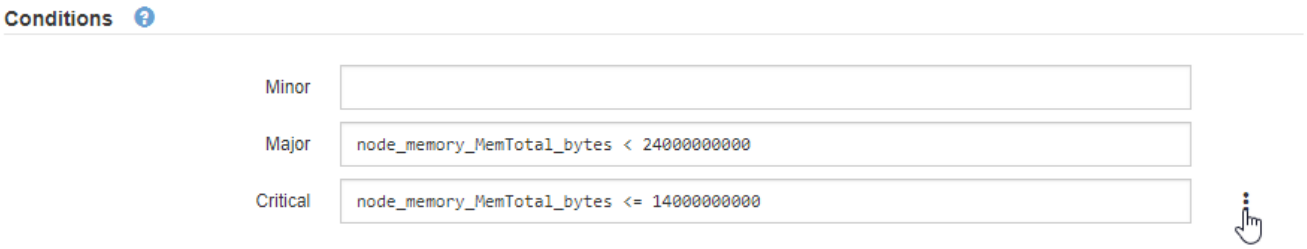
5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.

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

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

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

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



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

Uma expressão básica geralmente tem a seguinte forma:

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

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

Essa expressão faz com que um alerta seja acionado se a quantidade de RAM instalada em 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 durante o qual uma condição deve permanecer continuamente em vigor antes que o alerta seja acionado e selecione a unidade de tempo.

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

   O padrão é 5 minutos.

8. Selecione **Salvar**.

   Se você editou uma regra de alerta padrão, **Default** aparecerá na coluna Tipo. Se você desativou uma regra de alerta padrão ou personalizada, **Disabled** aparecerá na coluna **Status**.

Desative regras de alerta no StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Gerenciar 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 recomendável. Se uma regra de alerta estiver desativada, você pode não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

1. Selecione **Alertas** > **Regras**.

   A página Regras de Alerta é exibida.

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

   A caixa de diálogo Editar Regra é exibida.

4. Selecione ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está

atualmente habilitada.

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

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

5. Selecione **Salvar**.

   Desativado aparece na coluna **Status**.

Remova regras de alerta personalizadas no StorageGRID

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

Antes de começar

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

Passos

1. Selecione **Alertas** > **Regras**.

   A página Regras de Alerta é exibida.

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

   Não é possível remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

   Uma caixa de diálogo de confirmação é exibida.

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

   Qualquer instância ativa do alerta será resolvida em até 10 minutos.

Gerencie notificações de alerta

Configure as notificações SNMP para alertas do StorageGRID

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

Você pode usar a opção **Configuração** > **Monitoramento** > **Agente SNMP** no Grid Manager ou os endpoints SNMP da API de Gerenciamento de Grid para habilitar e configurar o agente SNMP do StorageGRID. O agente SNMP é compatível com todas as três versões do protocolo SNMP.

Para aprender como configurar o agente SNMP, consulte "Use o monitoramento SNMP".

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

enviadas:

- Traps são notificações enviadas pelo agente SNMP que não exigem confirmação do sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como o acionamento de um alerta. Traps são suportados em todas as três versões do SNMP.
- Os informs são semelhantes aos traps, mas exigem confirmação do sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará o inform até que uma confirmação seja recebida ou o valor máximo de tentativas seja atingido. Os informs são suportados no SNMPv2c e no SNMPv3.

As notificações de captura e informação são enviadas quando um alerta padrão ou personalizado é acionado em qualquer nível de severidade. Para suprimir as notificações SNMP de um alerta, você deve configurar um silenciamento para o alerta. Consulte "Silenciar notificações de alerta".

Se a sua implantação do StorageGRID incluir vários Nós de Administração, o Nó de Administração primário será o remetente preferencial para notificações de alerta, pacotes AutoSupport e traps e informs SNMP. Se o Nó de Administração primário ficar indisponível, as notificações serão enviadas temporariamente por outros Nós de Administração. Consulte "O que é um nó de administração?".

Configure notificações por e-mail para alertas do StorageGRID

Se você deseja receber notificações por e-mail quando alertas ocorrerem, precisa fornecer informações sobre seu servidor SMTP. Você também precisa inserir os endereços de e-mail dos destinatários das notificações de alerta.

Antes de começar

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

Sobre esta tarefa

A configuração de e-mail usada para notificações de alerta não é utilizada para 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 primário será o remetente preferencial para notificações de alerta, pacotes AutoSupport e traps e informs SNMP. Se o Nó de Administração primário ficar indisponível, as notificações serão enviadas temporariamente por outros Nós de Administração. Consulte "O que é um nó de administração?".

Passos

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

   A página de Configuração de E-mail aparece.

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

   As seções Servidor de e-mail (SMTP), Segurança da Camada de Transporte (TLS), Endereços de e-mail e Filtros aparecem.

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

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

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

4. Na seção Endereços de e-mail, insira os endereços de e-mail do remetente e de cada destinatário.
   a. No campo **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-mails ou pessoa que deve receber um e-mail quando ocorrer um alerta.

      Selecione o ícone de mais ➕ para adicionar destinatários.

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

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

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

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

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

   d. No campo **Chave Privada**, insira a chave privada para o certificado de cliente em codificação PEM não criptografada.

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

Se precisar editar as configurações de e-mail, selecione o ícone de lápis para atualizar este campo.

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

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

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

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

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

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

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

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

8. Selecione **Salvar**.

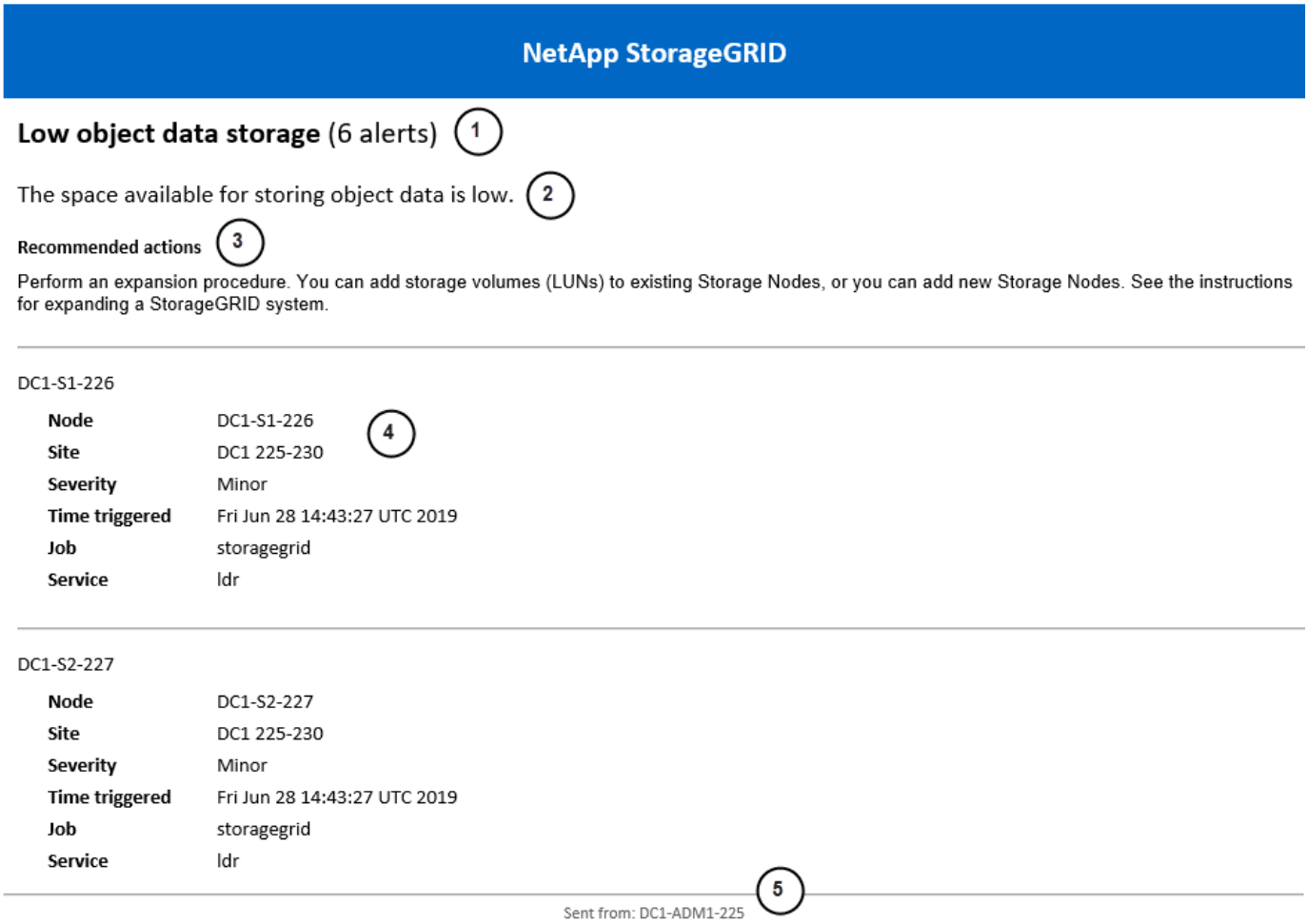
   O envio de um e-mail de teste não salva suas configurações. Você deve selecionar **Salvar**.

   As configurações de e-mail foram salvas.

Informações incluídas nas notificações de alerta por e-mail

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

As notificações por e-mail incluem as seguintes informações:



Chamada	Descrição
1	O nome do alerta, seguido pelo número de instâncias ativas desse 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 do trabalho e do serviço afetados.
5	O nome do host do nó de administração que enviou a notificação.

Como os alertas são agrupados

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

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

Comportamento	Exemplo
Cada notificação de alerta se aplica somente a alertas que possuem o mesmo nome. Se dois alertas com nomes diferentes forem acionados ao mesmo tempo, duas notificações por e-mail são enviadas.	• O alerta A é acionado em dois nós simultaneamente. Apenas uma notificação é enviada. • O alerta A é acionado no nó 1 e o alerta B é acionado no nó 2 ao mesmo tempo. Duas notificações são enviadas, uma para cada alerta.
Para um alerta específico em um nó específico, se os limites forem atingidos para mais de um nível de 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, StorageGRID aguarda 2 minutos antes de enviar uma notificação. Se outros alertas com o mesmo nome forem acionados durante esse período, 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 ocorrências do alerta.
Se outro alerta com o mesmo nome for acionado, StorageGRID aguarda 10 minutos antes de enviar uma nova notificação. A nova notificação reporta todos os alertas ativos (alertas atuais que não foram silenciados), mesmo que já 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 reportados.
Se houver vários alertas ativos com o mesmo nome e um deles for resolvido, uma nova notificação não será enviada caso o alerta volte a ocorrer no nó em que 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.
StorageGRID continua enviando notificações por e-mail a cada 7 dias até que todas as instâncias do alerta sejam resolvidas ou a regra de alerta seja silenciada.	1. O alerta A foi acionado para o nó 1 em 8 de março. Uma notificação é enviada. 2. O alerta A não foi resolvido nem silenciado. Notificações adicionais são enviadas em 15 de março, 22 de março, 29 de março e assim por diante.

Solucione problemas com notificações de alerta por e-mail

Se o alerta **Falha na notificação por e-mail** for acionado ou se você não conseguir receber a notificação de

alerta de teste por e-mail, siga estas etapas para resolver o problema.

Antes de começar

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

Passos

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

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

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

Silenciar notificações de alerta no StorageGRID

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

Antes de começar

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

Sobre esta tarefa

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

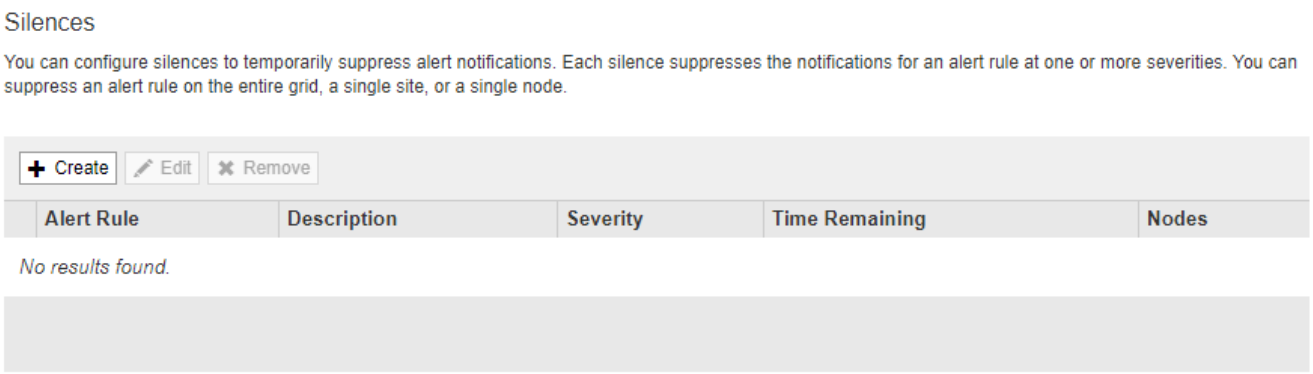
Se você habilitou o agente SNMP, o silenciamento também suprime traps e informs SNMP.

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

Passos

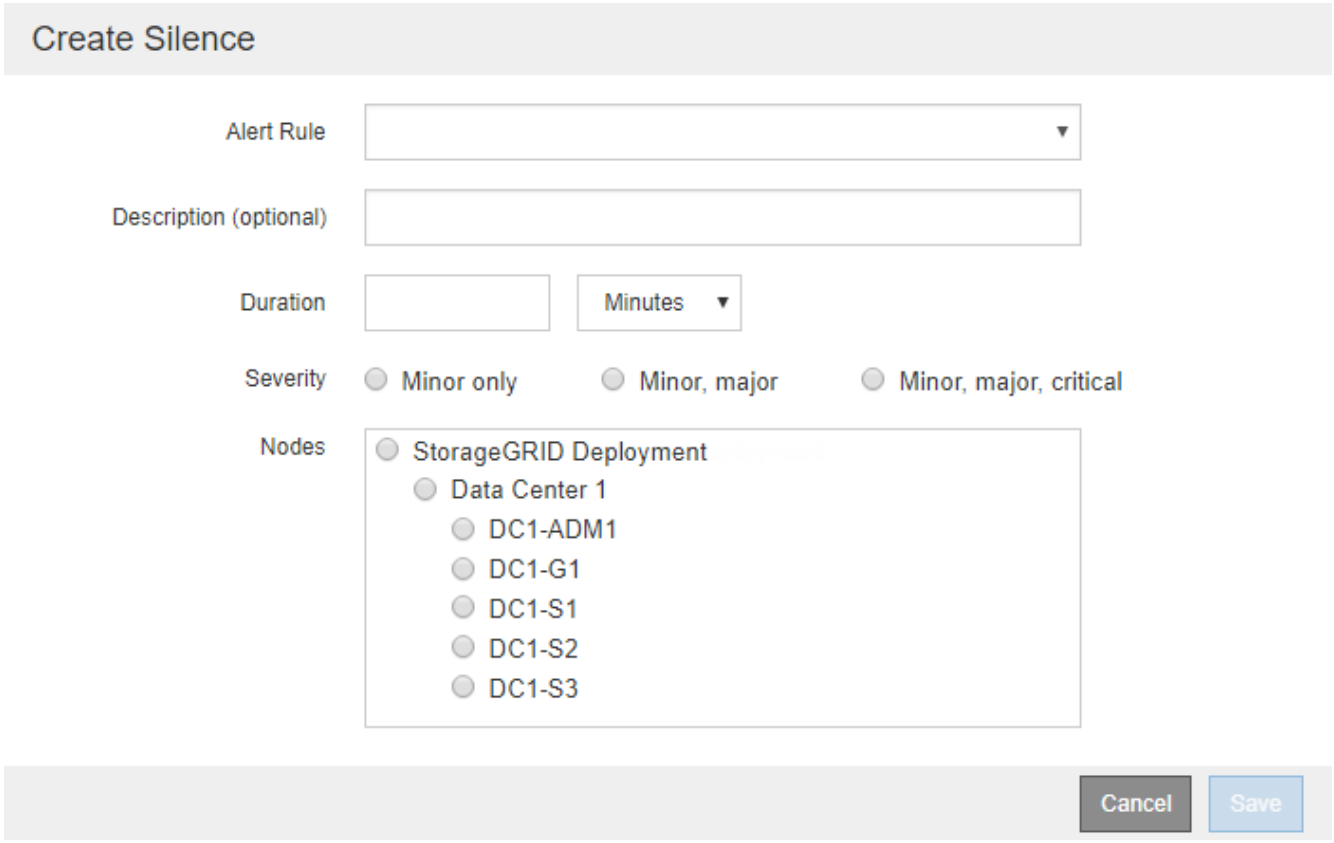
1. Selecione **Alertas** > **Silenciamentos**.

   A página Silences é exibida.



2. Selecione **Create**.

   A caixa de diálogo Criar Silence é exibida.



3. Selecione ou insira as seguintes informações:

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

Campo	Descrição
Descrição	Opcionalmente, uma descrição do silêncio. Por exemplo, descreva o propósito desse silêncio.
Duração	Por quanto tempo você deseja 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. Se uma regra de alerta for silenciada, você pode não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica. No entanto, pode ser necessário usar um silenciamento prolongado se um alerta for acionado por uma configuração específica e intencional, como pode ser o caso dos alertas **Services appliance link down** e **Storage appliance link down**.
Gravidade	Qual ou quais gravidades de alerta devem ser silenciadas. Se o alerta for acionado em uma das gravidades selecionadas, nenhuma notificação será enviada.
Nós	A qual nó ou nós você deseja que esse silenciamento se aplique. Você pode suprimir uma regra de alerta ou todas as regras em toda a grade, em um único site ou em um único nó. Se você selecionar toda a grade, o silenciamento se aplica a todos os sites e a todos os nós. Se você selecionar um site, o silenciamento se aplica somente aos nós desse site. **Observação:** Você não pode selecionar mais de um nó ou mais de um site para cada silenciamento. Você deve criar silenciamentos adicionais se quiser suprimir a mesma regra de alerta em mais de um nó ou mais de um site ao mesmo tempo.

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

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

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

Informações relacionadas

"Configurar o agente SNMP"

Alertas no StorageGRID

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 do sistema.

Alguns dos alertas padrão usam "Métricas Prometheus".

Alertas de appliance

${post_edited_translations.segment}	Descrição
Bateria do appliance expirada	A bateria do controlador de armazenamento do appliance expirou.
A bateria do appliance falhou	A bateria do controlador de armazenamento do aparelho apresentou defeito.
A bateria do appliance tem capacidade de aprendizado insuficiente	A bateria no controlador de armazenamento do appliance não possui capacidade de aprendizado suficiente.
Bateria do appliance perto do fim da vida útil	A bateria do controlador de armazenamento do aparelho está perto do fim de sua vida útil.
Bateria do appliance removida	A bateria do controlador de armazenamento do appliance está faltando.
A bateria do appliance está muito quente.	A bateria do controlador de armazenamento do aparelho está superaquecida.

${post_edited_translations.segment}	Descrição
Erro de comunicação BMC do appliance	A comunicação com o controlador de gerenciamento da placa-mãe (BMC) foi perdida.
Falha detectada no dispositivo de inicialização do appliance	Foi detectado um problema com o dispositivo de inicialização no appliance.
O dispositivo de backup de cache do appliance falhou	Um dispositivo de backup de cache persistente apresentou falha.
Dispositivo de backup de cache do appliance com capacidade insuficiente	A capacidade do dispositivo de backup em cache é insuficiente.
Dispositivo de backup de cache do appliance protegido contra gravação	Um dispositivo de backup em cache está protegido contra gravação.
Tamanho da memória cache do appliance incompatível	Os dois controladores do dispositivo possuem tamanhos de cache diferentes.
Falha na bateria CMOS do appliance	Foi detectado um problema com a bateria CMOS do appliance.
Temperatura muito alta no chassi do controlador de computação do appliance	A temperatura do controlador de computação em um StorageGRID appliance excedeu um limite nominal.
Temperatura da CPU do controlador de computação do appliance muito alta	A temperatura da CPU no controlador de computação de um StorageGRID appliance excedeu um limite nominal.
O controlador de computação do appliance precisa de atenção	Foi detectada uma falha de hardware no controlador de computação de um StorageGRID appliance.
A fonte de alimentação do controlador de computação do appliance A apresenta um problema	A fonte de alimentação A do controlador de computação apresenta um problema.
A fonte de alimentação B do controlador de computação do appliance apresenta um problema	A fonte de alimentação B no controlador de computação apresenta um problema.
O serviço de monitoramento de hardware de computação do appliance foi interrompido.	O serviço que monitora o status do hardware de armazenamento parou de funcionar.

${post_edited_translations.segment}	Descrição
Unidade DAS do appliance excedendo o limite de dados gravados por dia	Uma quantidade excessiva de dados está sendo gravada em uma unidade todos os dias, o que pode invalidar sua garantia.
Falha detectada na unidade DAS do appliance	Foi detectado um problema com uma unidade de armazenamento de conexão direta (DAS) no appliance.
A unidade DAS do appliance está no slot ou nó errado	Uma unidade de armazenamento de conexão direta (DAS) está no slot ou nó errado
Luz indicadora de localização da unidade DAS do appliance acesa	A luz indicadora de localização de uma ou mais unidades de armazenamento de conexão direta (DAS) em um Storage Node do dispositivo está acesa.
Reconstrução de unidades DAS do appliance	Uma unidade de armazenamento de conexão direta (DAS) está sendo reconstruída. Isso é esperado se ela foi substituída ou removida/reinserida recentemente.
Falha na ventoinha do dispositivo detectada	Foi detectado um problema com a unidade de ventilação do dispositivo.
Falha de Fibre Channel detectada no dispositivo de storage	Foi detectado um problema na ligação Fibre Channel entre o controlador de storage do dispositivo e o controlador de computação
Falha na porta HBA Fibre Channel do dispositivo de storage	Uma porta HBA Fibre Channel está com falha ou apresentou falha.
Unidades de cache flash do dispositivo de storage não estão otimizadas	Os discos utilizados para o cache SSD não são ideais.
Interconexão do dispositivo de storage/compartimento da bateria removido	O compartimento de interconexão/bateria está faltando.
Porta LACP do dispositivo ausente	Uma porta em um dispositivo de storage StorageGRID não está participando do vínculo LACP.
Falha na placa de interface de rede do dispositivo detectada	Foi detectado um problema com a placa de interface de rede (NIC) no dispositivo.
Fonte de alimentação geral do dispositivo de storage degradada	A potência de um dispositivo de storage StorageGRID está fora da tensão de operação recomendada.

${post_edited_translations.segment}	Descrição
É necessária uma atualização do software SANtricity OS para o dispositivo.	A versão do software SANtricity é inferior à versão mínima recomendada para esta release do StorageGRID.
Aviso crítico de SSD do dispositivo	Um SSD de dispositivo está relatando um aviso crítico.
Falha do controlador de armazenamento do dispositivo A	O controlador de armazenamento A em um dispositivo de storage StorageGRID apresentou falha.
Falha no controlador de storage do dispositivo B	O controlador de armazenamento B em um dispositivo de StorageGRID apresentou falha.
Falha na unidade controladora de storage do dispositivo	Uma ou mais unidades em um dispositivo de storage StorageGRID falharam ou não estão otimizadas.
Problema de hardware no controlador de armazenamento do dispositivo de storage	O software SANtricity está relatando "Necessita de atenção" para um componente em um dispositivo de StorageGRID.
Falha na fonte de alimentação do controlador de armazenamento do dispositivo de storage.	A fonte de alimentação A em um dispositivo de StorageGRID apresentou uma tensão de operação diferente da recomendada.
Falha na fonte de alimentação B do controlador de storage do dispositivo	A fonte de alimentação B em um dispositivo de storage StorageGRID apresentou uma tensão de operação diferente da recomendada.
Serviço de monitoramento de hardware de dispositivo de storage interrompido	O serviço que monitora o status do hardware de armazenamento parou de funcionar.
Prateleiras de dispositivos de storage degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de storage está degradado.
A temperatura do dispositivo de storage excedeu	A temperatura nominal ou máxima do controlador de storage do dispositivo foi excedida.
Sensor de temperatura do dispositivo de storage removido	Um sensor de temperatura foi removido.
Erro de inicialização segura UEFI do dispositivo	Um dispositivo não foi inicializado com segurança.
A entrada/saída de disco está muito lenta	A E/S de disco muito lenta pode estar impactando o desempenho do grid.

${post_edited_translations.segment}	Descrição
Falha no ventilador do dispositivo de storage detectada	Foi detectado um problema com uma ventoinha na controladora de armazenamento de um dispositivo de storage.
Conectividade de storage do dispositivo de storage degradada	Existe um problema com uma ou mais conexões entre o controlador de computação e o controlador de storage.
Dispositivo de storage inacessível	Não é possível acessar o dispositivo de storage.

Alertas de auditoria e syslog

${post_edited_translations.segment}	Descrição
Os registros de auditoria estão sendo adicionados à fila na memória	O nó não consegue enviar logs para o servidor syslog local e a fila na memória está ficando cheia.
Erro de encaminhamento do servidor syslog externo	O nó não consegue encaminhar logs para o servidor syslog externo.
Fila de auditoria grande	A fila de disco para mensagens de auditoria está cheia. Se essa condição não for resolvida, as operações S3 poderão falhar.
Os logs estão sendo adicionados à fila em disco	O nó não consegue encaminhar os logs para o servidor syslog externo e a fila em disco está ficando cheia.

Alertas de bucket

${post_edited_translations.segment}	Descrição
FabricPool bucket possui uma configuração de consistência de bucket não suportada	Um bucket FabricPool usa o nível de consistência Available ou Strong-site, que não é suportado.
FabricPool bucket possui uma configuração de versionamento não suportada	Um bucket FabricPool possui controle de versão ou S3 Object Lock ativados, que não são suportados.

Alertas Cassandra

${post_edited_translations.segment}	Descrição
Erro no compactador automático do Cassandra	O compactador automático Cassandra apresentou um erro.
Métricas de auto-compactador do Cassandra desatualizadas	As métricas que descrevem o auto-compactador do Cassandra estão desatualizadas.
Erro de comunicação do Cassandra	Os nós que executam o serviço Cassandra estão apresentando dificuldades de comunicação entre si.
Compactações de Cassandra sobrecarregadas	O processo de compactação do Cassandra está sobrecarregado.
Erro de gravação de tamanho excessivo do Cassandra	Um processo interno do StorageGRID enviou uma solicitação de gravação para o Cassandra que era muito grande.
Métricas de repair do Cassandra desatualizadas	As métricas que descrevem as tarefas de reparo do Cassandra estão desatualizadas.
Progresso do reparo do Cassandra lento	O progresso dos reparos no banco de dados Cassandra está lento.
Serviço de reparo Cassandra não disponível	O serviço de reparo do Cassandra não está disponível.
Corrupção da tabela Cassandra	O Cassandra detectou corrupção na tabela. O Cassandra reinicia automaticamente se detectar corrupção na tabela.

Alertas do Cloud Storage Pool

${post_edited_translations.segment}	Descrição
Erro de conectividade com o Cloud Storage Pool	A verificação de integridade dos Cloud Storage Pools detectou um ou mais novos erros.
Expiração da certificação da entidade final do IAM Roles Anywhere	O certificado da entidade final do IAM Roles Anywhere está prestes a expirar.

Alertas de replicação entre grids

${post_edited_translations.segment}	Descrição
Falha permanente na replicação entre grids	Ocorreu um erro de replicação entre grades que requer intervenção do usuário para resolver.
Recursos de replicação entre grades indisponíveis	As solicitações de replicação entre grades estão pendentes porque um recurso está indisponível.

Alertas DHCP

${post_edited_translations.segment}	Descrição
O lease DHCP expirou	O tempo de concessão DHCP em uma interface de rede expirou.
O prazo de concessão DHCP está prestes a expirar	O tempo de concessão DHCP em uma interface de rede está prestes a expirar.
Servidor DHCP indisponível	O servidor DHCP está indisponível.

Alertas de depuração e rastreamento

${post_edited_translations.segment}	Descrição
Depurar impacto no desempenho	Quando o modo de depuração está ativado, o desempenho do sistema pode ser afetado negativamente.
Configuração de rastreamento ativada	Quando a configuração de rastreamento está ativada, o desempenho do sistema pode ser afetado negativamente.

E-mail e alertas do AutoSupport

${post_edited_translations.segment}	Descrição
AutoSupport falha ao enviar a mensagem	A mensagem AutoSupport mais recente falhou ao ser enviada.
Falha na resolução do nome de domínio	O nó StorageGRID não conseguiu resolver nomes de domínio.
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail referente ao alerta.
Bucket de destino do arquivamento de logs não encontrado	O bucket de destino de arquivamento de logs está ausente, o que impede que os logs sejam arquivados no bucket de destino.

${post_edited_translations.segment}	Descrição
Erros de inform SNMP	Erros no envio de notificações SNMP inform para um destino de trap.
Acesso externo SSH ativado	O acesso externo via SSH está habilitado há mais de 24 horas.
Login SSH ou via console detectado	Nas últimas 24 horas, um usuário fez login com o Console Web ou SSH.

Alertas de codificação de apagamento (EC)

${post_edited_translations.segment}	Descrição
Falha de reequilíbrio de EC	O procedimento de reequilíbrio da EC falhou ou foi interrompido.
Falha de reparo EC	A tarefa de reparo dos dados de EC falhou ou foi interrompida.
Reparo de EC paralisado	Um processo de reparo de dados de EC foi interrompido.
Erro de verificação de fragmento codificado por apagamento	Fragmentos com código de apagamento não podem mais ser verificados. Fragmentos corrompidos podem não ser reparados.

Alertas de expiração de certificados

${post_edited_translations.segment}	Descrição
Expiração do certificado CA do proxy de administração	Um ou mais certificados no pacote de CA do servidor proxy administrativo estão prestes a expirar.
Expiração do certificado do cliente	Um ou mais certificados de cliente estão prestes a expirar.
Expiração do certificado global do servidor S3	O certificado global do servidor S3 está prestes a expirar.
Expiração do certificado do endpoint 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 da autoridade certificadora (CA) usado para assinar o certificado do servidor syslog externo está prestes a expirar.

${post_edited_translations.segment}	Descrição
Expiração do certificado do cliente syslog externo	O certificado do cliente para um servidor syslog externo está prestes a expirar.
Expiração do certificado do servidor syslog externo	O certificado do servidor apresentado pelo servidor syslog externo está prestes a expirar.

Alertas da rede Grid

${post_edited_translations.segment}	Descrição
Incompatibilidade de MTU na rede Grid	A configuração de MTU para a interface da Grid Network (eth0) difere significativamente entre os nós do grid.

Alertas de grid federation

${post_edited_translations.segment}	Descrição
Expiração do certificado de federação da grid	Um ou mais certificados de federação de grid estão prestes a expirar.
Falha na conexão da federação de grid	A conexão de federação de grid entre o grid local e o remoto não está funcionando.

Alertas de uso intenso ou alta latência

${post_edited_translations.segment}	Descrição
Uso elevado de heap Java	Uma alta porcentagem do espaço de heap de Java está sendo utilizada.
Alta latência para consultas de metadados	O tempo médio para consultas de metadados do Cassandra é muito longo.

Alertas de federação de identidades

${post_edited_translations.segment}	Descrição
Falha na sincronização da federação de identidades	Não foi possível sincronizar grupos e usuários federados da fonte de identidade.

${post_edited_translations.segment}	Descrição
Falha na sincronização da federação de identidades para um tenant	Não foi possível sincronizar grupos e usuários federados da fonte de identidade configurada por um tenant.

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

${post_edited_translations.segment}	Descrição
Colocação no ILM inatingível	Uma instrução de posicionamento em uma regra ILM não pode ser realizada para determinados objetos.
Taxa de varredura de ILM baixa	A taxa de varredura do ILM está definida para menos de 100 objetos/segundo.

Alertas do servidor de gerenciamento de chaves (KMS)

${post_edited_translations.segment}	Descrição
Expiração do certificado KMS CA	O certificado da autoridade certificadora (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Expiração do certificado do cliente KMS	O certificado de cliente para um servidor de gerenciamento de chaves está prestes a expirar
Falha ao carregar a configuração do KMS	A configuração do servidor de gerenciamento de chaves existe, mas falhou ao carregar.
Erro de conectividade KMS	Um nó do appliance não conseguiu se conectar ao servidor de gerenciamento de chaves do seu site.
Nome da chave de criptografia KMS não encontrado	O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido.
Falha na rotação da chave de criptografia KMS	Todos os volumes do dispositivo foram descriptografados com sucesso, mas um ou mais volumes não puderam ser rotacionados para a chave mais recente.
KMS não está configurado	Não existe um servidor de gerenciamento de chaves para este site.
A chave KMS não conseguiu descriptografar um volume do appliance.	Um ou mais volumes em um appliance com criptografia de nó ativada não puderam ser descriptografados com a chave KMS atual.

${post_edited_translations.segment}	Descrição
Expiração do certificado do servidor KMS	O certificado do servidor usado pelo servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Falha de conectividade com o servidor KMS	Um nó do appliance não conseguiu se conectar a um ou mais servidores no cluster de servidores de gerenciamento de chaves do seu site.

Alertas do balanceador de carga

${post_edited_translations.segment}	Descrição
Conexões de balanceador de carga com zero solicitações elevadas	Uma porcentagem elevada de conexões com os endpoints do balanceador de carga foi desconectada sem que as solicitações fossem executadas.

Alertas de deslocamento do relógio local

${post_edited_translations.segment}	Descrição
Grande diferença de horário do relógio local	A diferença entre o relógio local e o horário do Network Time Protocol (NTP) é muito grande.

Alertas de pouca memória ou pouco espaço em disco

${post_edited_translations.segment}	Descrição
Baixa capacidade de disco para log de auditoria	O espaço disponível para os logs de auditoria é baixo. Se essa condição não for resolvida, as operações do S3 poderão falhar.
Pouca memória disponível no nó	A quantidade de RAM disponível em um nó é baixa.
Pouco espaço livre para pool de storage	O espaço disponível para armazenar dados de objetos no Storage Node é baixo.
Pouca memória instalada no nó	A quantidade de memória instalada em um nó é baixa.
Armazenamento de metadados baixo	O espaço disponível para armazenar metadados de objetos é baixo.
Baixa capacidade de disco para métricas	O espaço disponível para o banco de dados de métricas está baixo.

${post_edited_translations.segment}	Descrição
Baixo storage de objetos	O espaço disponível para armazenar dados de objetos é baixo.
Substituição do limite inferior somente leitura	O limite de sobreposição da marca d'água de leitura flexível do volume de storage é menor que a marca d'água mínima otimizada para um Storage Node.
Baixa capacidade do disco raiz	O espaço disponível no disco raiz é baixo.
Baixa capacidade de dados do sistema	O espaço disponível em /var/local é baixo. Se essa condição não for resolvida, as operações S3 poderão falhar.
Pouco espaço livre no diretório tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de nó ou rede de nós

${post_edited_translations.segment}	Descrição
Quórum do ADC não atingido	O nó de armazenamento com serviço ADC está offline. As operações de expansão e desativação estão bloqueadas até que o quorum do ADC seja restaurado.
Uso recebido pela rede de administração	O uso de recebimento na Rede Administrativa está alto.
Uso de transmissão da rede administrativa	O uso de transmissão na Admin Network está alto.
Falha na configuração do firewall	Falha ao aplicar a configuração do firewall.
Pontos de extremidade da interface de gerenciamento em modo de contingência	Todos os endpoints da interface de gerenciamento estão utilizando as portas padrão como alternativa há muito tempo.
Erro de conectividade da rede do nó	Ocorreram erros durante a transferência de dados entre os nós.
Erro de quadro de recepção da rede do nó	Uma alta porcentagem dos quadros de rede recebidos por um nó apresentava erros.
Nó não está sincronizado com o servidor NTP	O nó não está sincronizado com o servidor NTP.
Nó não está bloqueado com o servidor NTP	O nó não está vinculado a um servidor NTP.

${post_edited_translations.segment}	Descrição
Rede do nó não-appliance inativa	Um ou mais dispositivos de rede estão inativos ou desconectados.
Link do appliance de serviços inativo na Admin Network	A interface do appliance com a Admin Network (eth1) está inativa ou desconectada.
Link do appliance de serviços inativo na porta 1 da Admin Network	A porta de rede Admin Network 1 do appliance está inativa ou desconectada.
Link do appliance de serviços inativo na Client Network	A interface do appliance com a rede do cliente (eth2) está inativa ou desconectada.
Link do appliance de serviços inativo na porta de rede 1	A porta de rede 1 do appliance está inativa ou desconectada.
Link do appliance de serviços inativo na porta de rede 2	A porta de rede 2 do appliance está inativa ou desconectada.
Link do appliance de serviços inativo na porta de rede 3	A porta de rede 3 do appliance está inativa ou desconectada.
Link do appliance de serviços inativo na porta de rede 4	A porta de rede 4 do appliance está inativa ou desconectada.
Link do appliance de storage inativo na Admin Network	A interface do appliance com a Admin Network (eth1) está inativa ou desconectada.
Link do storage appliance inativo na porta 1 da Admin Network	A porta de rede Admin Network 1 do appliance está inativa ou desconectada.
Link do appliance de storage inativo na Client Network	A interface do appliance com a rede do cliente (eth2) está inativa ou desconectada.
Link do appliance de storage inativo na porta de rede 1	A porta de rede 1 do appliance está inativa ou desconectada.
Link do storage appliance inativo na porta de rede 2	A porta de rede 2 do appliance está inativa ou desconectada.
Link do appliance de storage inativo na porta de rede 3	A porta de rede 3 do appliance está inativa ou desconectada.
Link do storage appliance inativo na porta de rede 4	A porta de rede 4 do appliance está inativa ou desconectada.

${post_edited_translations.segment}	Descrição
Nó de storage não está no estado de storage desejado	O serviço LDR em um nó de armazenamento não consegue fazer a transição para o estado desejado devido a um erro interno ou problema relacionado ao volume
Uso da conexão TCP	O número de conexões TCP neste nó está se aproximando do número máximo que pode ser rastreado.
Não foi possível se comunicar com o nó	Um ou mais serviços não estão respondendo ou o nó está inacessível.
Reinicialização inesperada do nó	Um nó foi reinicializado inesperadamente nas últimas 24 horas.

Alertas de objetos

${post_edited_translations.segment}	Descrição
A verificação de existência do objeto falhou	A verificação da existência do objeto falhou.
Verificação de existência do objeto travada	A tarefa de verificação da existência do objeto está parada.
Objetos potencialmente perdidos	Um ou mais objetos potencialmente perdidos do grid.
Objetos órfãos detectados	Objetos órfãos foram detectados.
O tamanho do objeto S3 PUT é muito grande	Um cliente está tentando realizar uma operação PUT Object que excede os limites de tamanho do S3.
Objeto corrompido não identificado detectado	Foi encontrado um arquivo no storage de objetos replicado que não pôde ser identificado como um objeto replicado.

Alertas de corrupção de objetos

${post_edited_translations.segment}	Descrição
Tamanho do objeto incompatível	Tamanho de objeto inesperado detectado durante o procedimento de verificação de existência do objeto.

Alertas de serviços da plataforma

${post_edited_translations.segment}	Descrição
A capacidade de solicitações pendentes dos Platform Services está baixa.	O número de solicitações pendentes nos Serviços da Plataforma está se aproximando da capacidade.
Serviços da plataforma indisponíveis	Há poucos nós de armazenamento com o serviço RSM em execução ou disponíveis em um site.

Alertas de volume de storage

${post_edited_translations.segment}	Descrição
O volume de storage precisa de atenção	Um volume de storage está offline e precisa de atenção.
O volume de storage precisa ser restaurado.	Um volume de storage foi recuperado e precisa ser restaurado.
Volume de armazenamento offline	Um volume de storage está offline há mais de 5 minutos.
Tentativa de remontagem do volume de storage	Um volume de armazenamento estava offline e acionou uma remontagem automática. Isso pode indicar um problema na unidade ou erros no sistema de arquivos.
A restauração do volume falhou ao iniciar o reparo dos dados replicados	Não foi possível iniciar automaticamente a reparação de dados replicados para um volume reparado.

Alertas de serviços StorageGRID

${post_edited_translations.segment}	Descrição
Serviço nginx usando configuração de backup	A configuração do serviço nginx é inválida. A configuração anterior está sendo utilizada.
Serviço nginx-gw usando configuração de backup	A configuração do serviço nginx-gw é inválida. A configuração anterior está sendo usada.
É necessário reiniciar para desativar FIPS	A política de segurança não exige o modo FIPS, mas os módulos FIPS estão em uso.
É necessário reiniciar para ativar FIPS	A política de segurança exige o modo FIPS, mas os módulos FIPS não estão em uso.

${post_edited_translations.segment}	Descrição
Serviço SSH usando configuração de backup	A configuração do serviço SSH é inválida. A configuração anterior está sendo utilizada.

Alertas de locatário

${post_edited_translations.segment}	Descrição
Alta utilização da quota do locatário	Uma alta porcentagem do espaço de cota está sendo utilizada. Essa regra está desativada por padrão porque pode gerar muitas notificações.

Métricas do Prometheus comumente usadas no StorageGRID

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

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

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

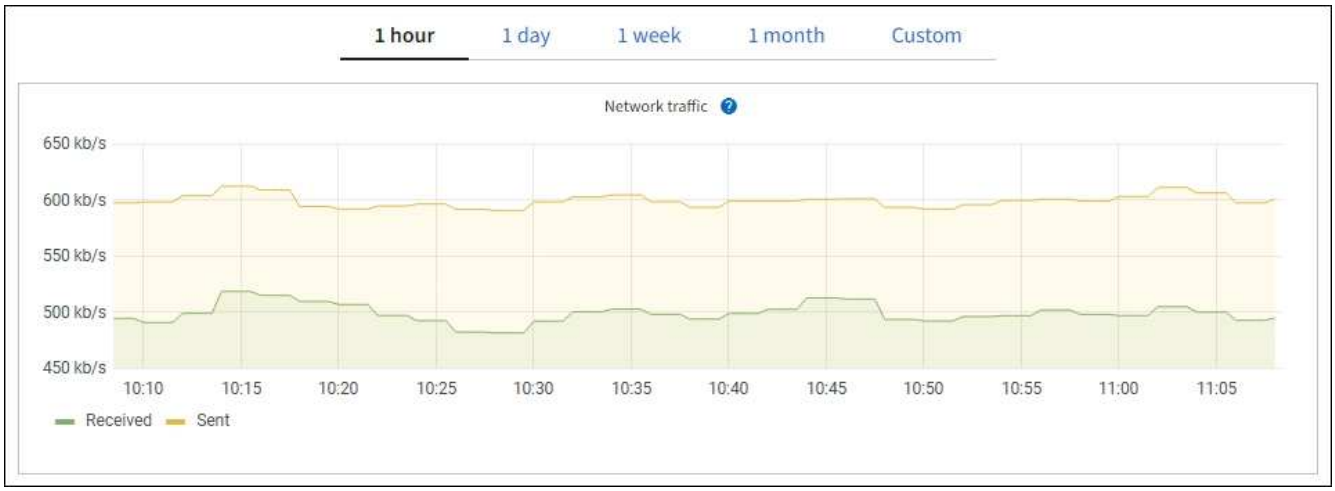
O que são métricas Prometheus?

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

Onde as métricas do Prometheus são utilizadas?

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

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



- **Alertas**: Os alertas são acionados em níveis de gravidade específicos quando as condições das regras de alerta que usam métricas Prometheus são avaliadas como verdadeiras.
- **API de Gerenciamento de Grid**: Você pode usar métricas do Prometheus em regras de alerta personalizadas ou com ferramentas de automação externas para monitorar seu sistema StorageGRID. Uma lista completa de métricas do Prometheus está disponível na API de Gerenciamento de Grid. (Na parte superior do Gerenciador de Grid, selecione o ícone de ajuda e selecione **API documentation** > **metrics**.) 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 destinam-se apenas ao uso interno e estão sujeitas a alterações entre versões do StorageGRID sem aviso prévio.

- As páginas **Suporte** > **Ferramentas** > **Diagnóstico** e **Suporte** > **Ferramentas** > **Métricas**: essas páginas, destinadas principalmente ao suporte técnico, fornecem diversas ferramentas e gráficos que utilizam os valores das métricas do Prometheus.

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

Lista das métricas mais comuns

A lista a seguir contém as métricas Prometheus mais usadas.

> 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.

bytes disponíveis no sistema de arquivos do nó

A quantidade de espaço do sistema de arquivos disponível para usuários não-root, em bytes.

node_memory_MemAvailable_bytes

Campo de informações de memória MemAvailable_bytes.

portadora de rede do nó

Valor portador de `/sys/class/net/iface`.

node_network_receive_errs_total

Estatística de dispositivo de rede `receive_errs`.

node_network_transmit_errs_total

Estatística de dispositivo de rede `transmit_errs`.

storagegrid_administrativamente_desativado

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

status_do_hardware_do_controlador_de_computação_da_appliance_StorageGRID

O status do hardware do controlador de computação em um appliance.

discos com falha do StorageGRID appliance

Para o controlador de armazenamento em um appliance, o número de unidades que não estão otimizadas.

status_do_hardware_do_controlador_de_armazenamento_da_appliance_StorageGRID

O status geral do hardware do controlador de armazenamento em um appliance.

storagegrid_content_buckets_and_containers

O número total de buckets S3 conhecidos por este Storage Node.

objetos_de_conteúdo_do_storagegrid

Número total de objetos de dados S3 conhecidos por este Storage Node. A contagem é válida apenas para objetos de dados criados por aplicativos cliente que interagem com o sistema por meio do S3.

storagegrid_content_objects_lost

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

"Solucionar problemas de dados de objetos perdidos ou ausentes"

storagegrid_http_sessions_incoming_attempted

O número total de sessões HTTP que foram tentadas em um Storage Node.

storagegrid_http_sessions_incoming_currently_established

O número de sessões HTTP que estão atualmente ativas (abertas) no Storage Node.

storagegrid_http_sessions_incoming_failed

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

storagegrid_http_sessions_incoming_successful

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

storagegrid_ilm_aguardando_objetos_em_fundo

Número total de objetos neste nó aguardando avaliação de ILM a partir da varredura.

storagegrid_ilm_aguardando_avaliação_do_cliente_objetos_por_segundo

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

storagegrid_ilm_aguardando_objetos_do_cliente

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

storagegrid_ilm_aguardando_total_objetos

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 verificados e enfileirados para ILM.

storagegrid_ilm_scan_period_estimated_minutes

Tempo estimado para concluir uma varredura ILM completa 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 endpoint do balanceador de carga em segundos desde a época.

storagegrid_metadata_queries_average_latency_milliseconds

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

storagegrid_network_received_bytes

Quantidade total de dados recebidos desde a instalação.

bytes_transmitidos_da_rede_StorageGRID

Quantidade total de dados enviados desde a instalação.

porcentagem de utilização da CPU do nó StorageGRID

A porcentagem de tempo de CPU disponível que está sendo usada por este serviço. Indica o nível de carga do serviço. A quantidade de tempo de CPU disponível depende do número de CPUs do servidor.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Desvio sistemático de tempo fornecido por uma fonte de tempo escolhida. O desvio é introduzido quando o atraso para alcançar uma fonte de tempo não é igual ao tempo necessário para a fonte de tempo alcançar o cliente NTP.

storagegrid_ntp_locked

O nó não está vinculado a um servidor de Network Time Protocol (NTP).

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

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

storagegrid_servercertificate_management_interface_cert_expiry_days

O número de dias antes do vencimento do certificado da interface de gerenciamento.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

O número de dias antes do vencimento do certificado da API de Object Storage.

storagegrid_service_cpu_seconds

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

uso de memória do serviço storagegrid_service_memory_usage_bytes

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

storagegrid_service_network_received_bytes

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.

reinicializações_do_serviço_StorageGRID

O número total de vezes que o serviço foi reiniciado.

storagegrid_service_runtime_seconds

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

storagegrid_service_uptime_seconds

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

storagegrid_storage_state_current

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

- 10 = Offline
- 15 = Manutenção
- 20 = Somente leitura
- 30 = Online

status_storagegrid_storage

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

- 0 = Sem erros

- 10 = Em Transição
- 20 = Espaço livre insuficiente
- 30 = Volume(s) indisponível(is)
- 40 = Erro

storagegrid_storage_utilization_data_bytes

Uma estimativa do tamanho total dos dados de objetos replicados e codificados para eliminação no Storage Node.

storagegrid_storage_utilization_metadata_allowed_bytes

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

storagegrid_storage_utilization_metadata_bytes

Quantidade de metadados de objetos no volume de storage 0, em bytes.

storagegrid_storage_utilization_total_space_bytes

A quantidade total de espaço de storage alocado a todos os object stores.

storagegrid_storage_utilization_usable_space_bytes

A quantidade total de espaço de storage de objetos restante. Calculada somando a quantidade de espaço disponível para todos os storages de objetos no Storage Node.

storagegrid_tenant_usage_data_bytes

O tamanho lógico de todos os objetos para o tenant.

storagegrid_tenant_usage_object_count

O número de objetos para o tenant.

storagegrid_tenant_usage_quota_bytes

A quantidade máxima de espaço lógico disponível para os objetos do locatário. Se nenhuma métrica de cota 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 Grid Management API.

Passos

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

Referência de arquivos de log

Arquivos de log do StorageGRID

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

Os logs são categorizados da seguinte forma:

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

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

Acesse os logs

Para acessar os logs, você pode "coletar arquivos de log e dados do sistema" de um ou mais nós como um único arquivo de log. Ou, você pode acessar arquivos de log individuais para cada nó da grid da seguinte forma:

Passos

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

Exportar registros para o servidor syslog

A exportação dos registros para o servidor syslog oferece as seguintes funcionalidades:

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

Para exportar os registros, consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

Categorias de arquivos de log

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

Local de arquivamento	Descrição
auditoria	Mensagens de auditoria geradas durante a operação normal do sistema.
logs do sistema operacional base	Informações básicas do sistema operacional, incluindo as versões da imagem StorageGRID.
pacotes	Informações de configuração global (bundles).
cache-svc	Logs de serviço de cache (somente em Gateway Nodes).
cassandra	Informações do banco de dados Cassandra e arquivos de log de reparo do Reaper.
ec	Informações do VCS sobre o nó atual e informações do grupo EC por ID de perfil.
grid	Registros gerais da grade, incluindo logs de depuração (`bycast.log` e `servermanager`logs.
grid.json	Arquivo de configuração compartilhado entre todos os nós. Além disso, `node.json` é específico para o nó atual.
hagroups	Métricas e arquivos de log de grupos de alta disponibilidade.
instalar	`Gdu-server` e instalar logs.
Lambda-arbitrator	Registros relacionados à solicitação de proxy S3 Select.
vazou	Registros do serviço leakd.
lumberjack.log	Mensagens de depuração relacionadas à coleta de log.
Métricas	Registros de serviço para Grafana, Jaeger, node exporter e Prometheus.
miscd	Registros de acesso miscd e erros.
mysql	A configuração do banco de dados mariaDB e os logs relacionados.
rede	Registros gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos de configuração e registros do balanceador de carga e da federação de grids. Inclui também registros de tráfego do Grid Manager e do Tenant Manager.

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

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

Registros do software StorageGRID

Você pode usar os registros do StorageGRID para solucionar problemas.

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

Registros gerais do StorageGRID

Nome do arquivo	Notas	Encontrado em
/var/local/log/bycast.log	O arquivo principal de solução de problemas do StorageGRID.	Todos os nós
/var/local/log/bycast-err.log	Contém um subconjunto de `bycast.log` (mensagens com gravidade ERRO e CRÍTICO). Mensagens CRÍTICAS também são exibidas no sistema.	Todos os nós
/var/local/core/	Contém quaisquer arquivos de despejo de memória criados caso o programa seja encerrado de forma anormal. Possíveis causas incluem falhas de asserção, violações ou tempos limite de thread. **Nota**: O arquivo `` `/var/local/core/kexec_cmd `` geralmente existe nos nós do appliance e não indica um erro.	Todos os nós

Registros relacionados à criptografia

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssh-config-generation.log	Contém registros relacionados à geração de configurações SSH e à reinicialização dos serviços SSH.	Todos os nós
/var/local/log/nginx/config-generation.log	Contém registros relacionados à geração de configurações do nginx e à recarga dos serviços do nginx.	Todos os nós
/var/local/log/nginx-gw/config-generation.log	Contém registros relacionados à geração de configurações do nginx-gw (e à recarga dos serviços do nginx-gw).	Nós de administração e gateway
/var/local/log/update-cipher-configurations.log	Contém registros relacionados à configuração de políticas TLS e SSH.	Todos os nós

Registros de federação de grid

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

Logs do NMS

Nome do arquivo	Notas	Encontrado em
/var/local/log/nms.log	• Captura notificações do Grid Manager e do Tenant Manager. • Captura eventos relacionados à operação do serviço NMS. Por exemplo, notificações por e-mail e alterações de configuração. • Contém atualizações de pacotes XML resultantes de alterações de configuração feitas no sistema. • Contém mensagens de erro relacionadas à redução da amostragem de atributos realizada uma vez por dia. • Contém mensagens de erro do servidor web Java, por exemplo, erros de geração de página e erros de status HTTP 500. • Contém registros relacionados a AutoSupport.	Nós de administração
/var/local/log/nms.errlog	Contém mensagens de erro relacionadas a atualizações do banco de dados MySQL. Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Existe 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 arquivo	Notas	Encontrado em
/var/local/log/servermanager.log	Arquivo de log do aplicativo Server Manager em execução no servidor.	Todos os nós
/var/local/log/GridstatBackend.errlog	Arquivo de log do aplicativo de backend da GUI do Server Manager.	Todos os nós
/var/local/log/gridstat.errlog	Arquivo de log da interface gráfica do Server Manager.	Todos os nós

Registros de serviços do StorageGRID

Nome do arquivo	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/adc.errlog	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Existe um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de armazenamento executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Logs do serviço de cache.	Nós de gateway
/var/local/log/cassandra/system.log	Informações para o repositório de metadados (banco de dados Cassandra) que podem ser usadas caso ocorram problemas ao adicionar novos Storage Nodes ou se a tarefa de reparo do nodetool travar.	Nós de armazenamento
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que realiza reparos nos dados do banco de dados Cassandra.	Nós de armazenamento
/var/local/log/cassandra-reaper.errlog	Informações sobre erros do serviço Cassandra Reaper.	Nós de armazenamento
/var/local/log/chunk.errlog		Nós de armazenamento
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Este arquivo de log pode estar presente em sistemas que foram atualizados de uma versão anterior do StorageGRID. Ele contém informações antigas.	Nós de armazenamento
/var/local/log/dds.errlog		Nós de armazenamento
/var/local/log/dmv.errlog		Nós de armazenamento

Nome do arquivo	Notas	Encontrado em
/var/local/log/dynip*	Contém registros relacionados ao serviço dynip, que monitora a grid em busca de alterações dinâmicas de IP e atualiza a configuração local.	Todos os nós
/var/local/log/grafana.log	O arquivo de log associado ao serviço Grafana, que é usado para visualização de métricas no Grid Manager.	Nós de administração
/var/local/log/hagroups.log	O arquivo de log associado a grupos de alta disponibilidade.	Nós de administração e nós de gateway
/var/local/log/hagroups_events.log	Monitora mudanças de estado, como a transição de BACKUP para MASTER ou FAULT.	Nós de administração e nós de gateway
/var/local/log/idnt.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/jaeger.log	O log associado ao serviço jaeger, que é usado para coleta de rastreamento.	Todos os nós
/var/local/log/kstn.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/lambda*	Contém os logs do serviço S3 Select.	Nós de administração e gateway Apenas determinados nós de administração e gateway contêm este registro. Consulte o "Requisitos e limitações do S3 Select para nós de administração e gateway".
/var/local/log/ldr.errlog		Nós de armazenamento
/var/local/log/miscd/*.log	Contém registros do 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

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

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssm.errlog		Todos os nós
/var/local/log/update-s3vs-domains.log	Contém registros relacionados ao processamento de atualizações para a configuração de nomes de domínio virtuais hospedados no S3. Consulte as instruções para implementar aplicativos cliente do S3.	Nós de administração e gateway
/var/local/log/update-snmp-firewall.*	Contém registros relacionados às portas do firewall que estão sendo gerenciadas para SNMP.	Todos os nós
/var/local/log/update-sysl.log	Contém registros relacionados a alterações feitas na configuração do syslog do sistema.	Todos os nós
/var/local/log/update-traffic-classes.log	Contém registros relacionados a alterações na configuração dos classificadores de tráfego.	Nós de administração e gateway
/var/local/log/update-utcn.log	Contém registros relacionados ao modo de rede de cliente não confiável neste nó.	Todos os nós

Informações relacionadas

- "Sobre o bycast.log"
- "Utilize a API REST S3"

Registros de implantação e manutenção no StorageGRID

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

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

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

Saiba mais sobre o bycast.log do StorageGRID

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

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

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais de registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo está configurado. Consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

Rotação de arquivo 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 nomeado `bycast.log`. Quando o novo `bycast.log` atinge 1 GB, `bycast.log.1` é renomeado e descompactado para se 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 22ª versão 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 no mesmo local em que foi gravado. Descompactar o arquivo no mesmo local pode interferir nos scripts de rotação de log.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais de registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo está configurado. Consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

Informações relacionadas

"Coletar arquivos de log e dados do sistema"

Mensagens em bycast.log

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

Exemplo de mensagem ADE:

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

As mensagens ADE contêm as seguintes informações:

Segmento da mensagem	Valor no exemplo
ID do 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.uuuuuu)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: a verificação de integridade do volume 3 falhou com o motivo 'TOUT'

Gravidade das mensagens em bycast.log

As mensagens em `bycast.log` são atribuídas a níveis de gravidade.

Por exemplo:

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

Códigos de erro em `bycast.log`

A maioria das mensagens de erro em `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	Sem erro
GERR	Desconhecido
CANCELAR	Cancelado
ABRT	Abortado
TOUT	Tempo esgotado
INVL	Inválido
NFND	Não encontrado
VERSÃO	Versão
CONF	Configuração
FALHA	Falha
ICPL	Incompleto
FEITO	Feito
SUNV	Serviço indisponível

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

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

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

Número do erro	Código de erro	Significado
027	EFBIG	Arquivo muito grande
028	ENOSPC	Sem espaço disponível no dispositivo
029	ESPIPE	Busca ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Muitos links
032	EPIPE	Pipe quebrado
033	EDOM	Argumento matemático fora do domínio da função
034	ERANGE	Resultado matemático não representável
035	EDEADLK	Ocorreu um impasse de recursos
036	ENAMETOOLONG	Nome do arquivo muito longo
037	ENOLCK	Não há bloqueios de registro disponíveis
038	ENOSYS	Função não implementada
039	ENOTEMPTY	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
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Reinicialização de nível 3
048	ELNRNG	Número do link fora do intervalo

Número do erro	Código de erro	Significado
049	EUNATCH	Driver de protocolo não anexado
050	ENOCSI	Nenhuma estrutura CSI disponível
051	EL2HLT	Nível 2 interrompido
052	EBADE	Troca inválida
053	EBADR	Descritor de solicitação inválido
054	EXFULL	Exchange completo
055	ENOANO	Sem ânodo
056	EBADRQC	Código de solicitação inválido
057	EBADSLT	Slot inválido
058		
059	EBFONT	Formato de arquivo de fonte inválido
060	ENOSTR	Dispositivo não é um stream
061	ENODATA	Não há dados disponíveis
062	ETIME	O cronômetro expirou
063	ENOSR	Sem recursos de streams
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado
066	EREMOTE	O objeto é remoto
067	ENOLINK	O link foi cortado
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação ao enviar

Número do erro	Código de erro	Significado
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 muito grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em estado inválido
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	Tentativa de vincular muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	REINÍCIO	A chamada de sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro no pipe de Streams
087	EUSERS	Usuários em excesso
088	ENOTSOCK	Operação de soquete em não soquete
089	EDESTADDRREQ	Endereço de destino obrigatório
090	EMSGSIZE	Mensagem muito longa

Número do erro	Código de erro	Significado
091	EPROTOTYPE	Protocolo do 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 ponto de extremidade 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 fora do ar
101	ENETUNREACH	A rede está inacessível
102	ENETRESET	A conexão de rede foi interrompida devido a reinicialização
103	ECONNABORTED	O software causou o encerramento da conexão
104	ECONNRESET	Conexão reiniciada pelo peer
105	ENOBUFS	Sem espaço de buffer disponível
106	EISCONN	O endpoint de transporte já está conectado
107	ENOTCONN	O ponto de extremidade de transporte não está conectado
108	DESLIGAMENTO	Não é possível enviar após o encerramento do endpoint de transporte
109	ETOOMANYREFS	Muitas referências: não é possível concatenar
110	ETIMEDOUT	A conexão expirou

Número do erro	Código de erro	Significado
111	ECONNREFUSED	Conexão recusada
112	EHOSTDOWN	O host está inativo
113	EHOSTUNREACH	Não há rota para o host
114	EALREADY	Operação já em andamento
115	EINPROGRESS	Operação em andamento
116		
117	EUCLEAN	A estrutura precisa ser limpa.
118	ENOTNAM	Não é um arquivo de tipo nomeado XENIX
119	DISPONÍVEL	Não há semáforos XENIX disponíveis
120	EISNAM	É um arquivo de tipo nomeado
121	EREMOTEIO	Erro de E/S remota
122	EDQUOT	Cota excedida
123	ENOMEDIUM	Nenhum meio encontrado
124	EMEDIUMTYPE	Tipo de meio errado
125	CANCELADO	Operação cancelada
126	ENOKEY	A chave necessária não está disponível
127	EKEYEXPIRED	A chave expirou
128	EKEYREVOKED	A chave foi revogada
129	EKEYREJECTED	A chave foi rejeitada pelo serviço
130	EOWNERDEAD	Para mutexes robustos: proprietário faleceu
131	ENOTRECOVERABLE	Para mutexes robustos: estado não recuperável

Configurar o gerenciamento de logs e o servidor syslog externo

Servidores syslog externos no StorageGRID

Um servidor syslog externo é um servidor fora do StorageGRID que você pode usar para coletar informações de auditoria do sistema em um único local. Usar um servidor syslog externo permite que você reduza o tráfego de rede nos seus Nós de Administração e gerencie as informações com mais eficiência. Para StorageGRID, o formato do pacote de mensagem syslog de saída está em conformidade com a RFC 3164.

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

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

Quando usar um servidor syslog externo

Um servidor syslog externo é especialmente útil se você tiver uma grande grid, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. Enviar 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 de forma mais eficiente.
- Reduza o tráfego de rede em seus Nós de Administração, pois as informações de auditoria são transferidas diretamente dos diversos Nós de Armazenamento para o servidor syslog externo, sem precisar passar por um Nó de Administração.

> Quando os logs são enviados para um servidor syslog externo, logs individuais com mais de 8.192 bytes são truncados no final da mensagem para se adequarem às limitações comuns nas implementações de servidores syslog externos.

> Para maximizar as opções de recuperação de dados completas 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, consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

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

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

- **Chave privada do cliente**: Chave privada para o certificado do cliente em codificação PEM.

> Se você usar um certificado de cliente, também deverá usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, também deverá fornecer a senha. Não há benefício significativo em termos de segurança ao usar uma chave privada criptografada, pois a chave e a senha precisam ser armazenadas; por simplicidade, recomenda-se o uso de uma chave privada não criptografada, se disponível.

Como estimar o tamanho do servidor syslog externo

Normalmente, sua grid é dimensionada para atingir a taxa de transferência necessária, definida em termos de operações S3 por segundo ou bytes por segundo. Por exemplo, você pode ter o requisito de que sua grid processe 1.000 operações S3 por segundo, ou 2.000 MB por segundo, de ingestão e recuperação de objetos. Você deve dimensionar seu servidor syslog externo de acordo com os requisitos de dados da sua grid.

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

Use operações S3 por segundo em fórmulas de estimativa

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

> As fórmulas para dimensionamento de servidores syslog externos nas seções a seguir fornecem estimativas para casos comuns (e não para o pior cenário). Dependendo da sua configuração e carga de trabalho, você pode observar uma taxa de mensagens syslog ou um volume de dados syslog maior ou menor do que o previsto pelas fórmulas. 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 operações S3 por segundo que sua grid deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará processar usando as seguintes fórmulas, considerando que você mantenha os Níveis de Auditoria definidos com os valores padrão (todas as categorias definidas como Normal, exceto Storage, que está definida como Error):

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

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

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

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

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

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

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

Se você conseguir determinar os valores de P e K, poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará processar usando as seguintes fórmulas, considerando que você mantenha os Níveis de Auditoria definidos como padrão (todas as categorias definidas como Normal, exceto Storage, que está definida como Error):

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

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

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para os logs de auditoria pressupõem o uso das configurações padrão de nível de auditoria (todas as categorias definidas como Normal, exceto Storage, que está definida como Error). Fórmulas detalhadas para estimar a taxa e o tamanho médio das mensagens de auditoria para configurações de nível de auditoria diferentes das 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 os logs de auditoria, mas esteja ciente de que é provável que resulte em uma superestimação, pois as

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

Condição	Fórmula
Replicação: todos os níveis de auditoria definidos como Depuração ou Normal	Taxa de log de auditoria = 8 x Taxa de operações S3
Codificação de apagamento: todos os níveis de log de auditoria definidos como Depuração 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 esses motivos, 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 operações S3 por segundo que sua grid deve suportar, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo precisará processar usando as seguintes fórmulas:

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

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

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

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

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

Exemplos de estimativas de dimensionamento

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

- Replicação
- Codificação de apagamento

Se você usa replicação para proteção de dados

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

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

Se você conseguir determinar os valores de P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo precisará ser capaz de processar usando as seguintes fórmulas.

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

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

Se você utiliza codificação de apagamento para proteção de dados

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

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

Se você conseguir determinar os valores de P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo precisará ser capaz de processar usando as seguintes fórmulas.

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

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

Configure o gerenciamento de logs no StorageGRID

Conforme necessário, configure os níveis de auditoria, os cabeçalhos de protocolo e a localização das mensagens e logs de auditoria.

Todos os nós do StorageGRID geram mensagens de auditoria e logs para rastrear a atividade e os eventos do sistema. As mensagens de auditoria e os logs são ferramentas essenciais para monitoramento e solução de problemas.

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso de manutenção ou root".
- Se você planeja configurar um servidor syslog externo, você revisou e seguiu o "Considerações para usar um servidor syslog externo".
- Se você planeja configurar um servidor syslog externo usando o protocolo TLS ou RELP/TLS, você precisa ter a CA do servidor, os certificados do cliente e a chave privada do cliente necessários.

Alterar os níveis das mensagens de auditoria

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

Categoria de auditoria	Configuração padrão	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"
Storage	Erro	"Mensagens de auditoria de storage de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gerenciamento"

Categoria de auditoria	Configuração padrão	Mais informações
Leituras do cliente	Normal	"Mensagens de leitura do log de auditoria do cliente"
O cliente escreve	Normal	"Cliente escreve mensagens de log de auditoria"
ILM	Normal	"Mensagens de auditoria ILM"
Replicação entre grades	Erro	"CGRR: Solicitação de Replicação entre Grids"

Durante as atualizações, as configurações de nível de auditoria não terão efeito imediato.

Passos

1. Selecione **Configuração** > **Monitoramento** > **Gerenciamento de logs**.
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	Apenas as mensagens de erro são registradas — mensagens de log de auditoria para as quais o código de resultado não foi "successful" (SUCS).
Normal	As mensagens transacionais padrão são registradas: as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível se comporta da mesma forma que o nível de auditoria Normal.

As mensagens incluídas em um determinado nível abrangem aquelas que seriam registradas nos níveis superiores. Por exemplo, o nível Normal inclui todas as mensagens de erro.

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

3. Selecione **Salvar**.

Defina os cabeçalhos de solicitação HTTP

Opcionalmente, você pode definir quaisquer cabeçalhos de solicitação HTTP que desejar incluir nas mensagens de log de auditoria de leitura e gravação do cliente.

Passos

1. Na seção **Cabeçalhos do protocolo de auditoria**, defina os cabeçalhos de solicitação HTTP que você

deseja incluir nas mensagens de auditoria de leitura e gravação do cliente.

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

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

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

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

3. Selecione **Save**

Configurar local do log

Por padrão, as mensagens de auditoria e os logs são salvos nos nós onde são gerados. Eles são rotacionados periodicamente e, eventualmente, excluídos para evitar que consumam espaço de disco excessivo. Se você quiser salvar as mensagens de auditoria e um subconjunto dos logs externamente, usar um servidor syslog externo.

Se você deseja salvar os arquivos de log internamente, escolha um locatário e um bucket para storage de logs e habilite o arquivamento de logs.

Usar um servidor syslog externo

Opcionalmente, você pode configurar um servidor syslog externo para salvar log de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora do seu grid.

> Se você não quiser usar um servidor syslog externo, ignore esta etapa e vá para Selecione o local do log.

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

Insira as informações do syslog

Acesse o assistente Configurar servidor syslog externo e forneça as informações necessárias para que o StorageGRID acesse o servidor syslog externo.

Passos

1. Na guia Nó local e servidor externo, selecione **Configurar servidor syslog externo**. Ou, se você já configurou um servidor syslog externo anteriormente, selecione **Editar servidor syslog externo**.

   O assistente Configurar servidor syslog externo é exibido.

2. Na etapa **Inserir informações do syslog** do assistente, insira um domínio totalmente qualificado ou um endereço IPv4 ou IPv6 válido para o servidor syslog externo no campo **Host**.

3. Insira a porta de destino no servidor syslog externo (deve ser um número inteiro entre 1 e 65535). A porta padrão é 514.
4. Selecione o protocolo usado para enviar informações de auditoria para o servidor syslog externo.

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

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

   > ⓘ O Protocolo de Registro de Eventos Confiável (RELP) amplia a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. Usar o RELP pode ajudar a evitar a perda de informações de auditoria caso seu servidor syslog externo precise ser reiniciado.

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

      Uma marca de seleção verde aparece ao lado do nome do arquivo de certificado ou chave, notificando você de que o upload foi realizado com sucesso.

7. Selecione **Continue**.

Gerencie o conteúdo do syslog

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

Passos

1. Na etapa **Gerenciar conteúdo do syslog** do assistente, selecione cada tipo de informação de auditoria que você 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 fazer login ou quando um usuário faz login como root
   - **Enviar registros do aplicativo**: Envia "Arquivos de log do software StorageGRID" informações úteis para a resolução de problemas, incluindo:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Apenas nós de administração)
     - `prometheus.log`
     - `raft.log`

        - `hagroups.log`
    - **Enviar logs de acesso**: Envia logs de acesso HTTP para solicitações externas ao Grid Manager, Tenant Manager, endpoints de balanceador de carga configurados e solicitações de federação de grid de sistemas remotos.
2. Utilize os menus suspensos para selecionar a gravidade e a facility (tipo de mensagem) para cada categoria de informação de auditoria que você deseja enviar.

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

   a. Para **Severity**, selecione **Passthrough** ou selecione um valor de gravidade entre 0 e 7.

      Se você selecionar um valor, ele será aplicado a todas as mensagens desse tipo. As informações sobre diferentes níveis de gravidade serão perdidas se você substituir a gravidade por um valor fixo.

Gravidade	Descrição
Passthrough	Cada mensagem enviada para o syslog externo terá o mesmo valor de severidade que tinha 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 os logs de aplicativos, a gravidade varia entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA resulta em um valor "info", enquanto interromper intencionalmente o serviço SSM ou RSM resulta em um valor "notice". • Para os registros de acesso, a gravidade é "info".
0	Emergência: o sistema está inutilizável
1	Alerta: é preciso agir imediatamente
2	Crítico: condições críticas
3	Erro: condições de erro
4	Aviso: condições de alerta
5	Aviso: condição normal, porém significativa
6	Informativo: mensagens informativas
7	Depuração: mensagens de nível de depuração

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

Se você selecionar um valor, ele será aplicado a todas as mensagens desse tipo. As informações sobre diferentes facilities serão perdidas se você substituir facility por um valor fixo.

Instalação	Descrição
Passthrough	Cada mensagem enviada para o syslog externo deve ter o mesmo valor de facility que tinha quando foi registrada localmente no nó: • Para logs de auditoria, o recurso enviado para o servidor syslog externo é "local7". • Para eventos de segurança, os valores de facility são gerados pela distribuição Linux nos nós. • Para os logs de aplicação, os logs de aplicação enviados para o servidor syslog externo possuem os seguintes valores de facility: ◦ `bycast.log`: usuário ou daemon ◦ `bycast-err.log`: usuário, daemon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Para os registros de acesso, a facilidade enviada para o servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	usuário (mensagens de nível de usuário)
2	e-mail
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias da rede)
8	UUCP
9	cron (daemon de relógio)

Instalação	Descrição
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (log de auditoria)
14	logalert (alerta de log)
15	relógio (daemon do clock)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selecione **Continue**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós da sua grid enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudar a validar toda a sua infraestrutura de coleta de logs antes de enviar dados para o servidor syslog externo.

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

Passos

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

   Uma faixa verde indica que a configuração foi salva.

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

   Os resultados dos testes aparecem continuamente na página até que você interrompa o teste. Enquanto o teste está em andamento, suas mensagens de auditoria continuam sendo enviadas para seus destinos previamente configurados.

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

   Consulte "Solucione problemas em um servidor syslog externo" para ajudar você a resolver quaisquer erros.

4. Aguarde até ver uma faixa verde indicando que todos os nós passaram nos testes.
5. Verifique seu servidor syslog para determinar se as mensagens de teste estão sendo recebidas e processadas conforme o esperado.

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

6. Selecione **Parar e finalizar**.

   Você retorna para a página **Audit and syslog server**. Uma faixa 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 o local do log

Você pode especificar para onde os logs de auditoria, os logs de eventos de segurança "Registros de aplicativos StorageGRID" e os logs de acesso são enviados.

> StorageGRID usa por padrão destinos de auditoria de nós locais e armazena as informações de auditoria em `/var/local/log/localaudit.log`.
>
> Ao usar `/var/local/log/localaudit.log`, as entradas do log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um Storage Node. Você pode descobrir qual nó possui as entradas mais recentes usando o comando `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.
>
> Alguns destinos estão disponíveis somente se você tiver configurado um servidor syslog externo.

Passos

1. Selecione **Local de log** > **Nó local e servidor externo**.
2. Para alterar o local do log para os tipos de log, selecione uma opção diferente.

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

Opção	Descrição
Apenas nós locais (padrão)	As mensagens de auditoria, os logs de eventos de segurança e os logs de aplicativos não são enviados para os Admin Nodes. Em vez disso, elas são salvas apenas nos nós que as geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas em `/var/local/log/localaudit.log`. **Nota**: StorageGRID remove periodicamente os logs locais em um sistema de 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 22ª versão do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó. Para armazenar logs por um período prolongado, Use um locatário e um bucket para armazenamento de logs.
Nós administrativos/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 os logs de aplicativos são armazenados nos nós que os geraram. As informações de auditoria são armazenadas nos seguintes arquivos: • Nós de administração (primário e não primário): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo geralmente está vazio ou ausente. Pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais (`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é habilitada depois que você configurou um servidor syslog externo.
Nós de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (`/var/local/audit/export/audit.log` nos 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 habilitada depois que você configurou um servidor syslog externo.

3. Selecione **Salvar**.

   Uma mensagem de aviso aparece.

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

   Novos logs são enviados para os destinos que você selecionou. Os logs existentes permanecem em sua

localização atual.

Use um bucket

Os logs são rotacionados periodicamente. Use um bucket S3 na mesma grid para armazenar logs por um período prolongado.

1. Selecione **Local de log** > **Usar um bucket**.
2. Selecione a caixa de seleção **Enable archive logs**.
3. Se o locatário e o bucket listados não forem os que você deseja usar, selecione **Alterar locatário e bucket** e, em seguida, selecione **Criar locatário e bucket** ou **Selecionar locatário e bucket**.

   Criar locatário e bucket

   a. Insira um novo nome de locatário.
   b. Digite e confirme uma senha para o novo tenant.
   c. Insira um novo nome para o bucket.
   d. Selecione **Criar e ativar**.

   Selecione o locatário e o bucket

   a. Selecione o nome do locatário na lista suspensa.
   b. Selecione um bucket no menu suspenso.
   c. Selecione **Selecionar e ativar**.

4. Selecione **Salvar**.

   Os registros serão armazenados no locatário e no bucket que você especificou. O nome da chave do objeto para os registros tem este formato:

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   Por exemplo:

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```

Use o monitoramento SNMP

Use o monitoramento SNMP no StorageGRID

Se você deseja monitorar StorageGRID usando o Protocolo Simples de Gerenciamento de Rede (SNMP), você deve configurar o agente SNMP que está incluído com o StorageGRID.

- "Configurar o agente SNMP"
- "Atualize o agente SNMP"

Capacidades

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

Veja "Acesse os arquivos MIB" se você deseja baixar os arquivos MIB nos nós da sua grid.

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 exigem confirmação do sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como o acionamento de um alerta.

Traps são suportados em todas as três versões do SNMP.

Informa

Os informs são semelhantes aos traps, mas exigem confirmação do sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará o inform até que uma confirmação seja recebida ou o valor máximo de tentativas seja atingido.

Informs são suportados em SNMPv2c e SNMPv3.

As notificações de trap e inform são enviadas nos seguintes casos:

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

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

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	String comunitária	String comunitária	Usuário do Modelo de Segurança Baseado no Usuário (USM)
Notificações (TRAP e INFORM)	Apenas traps	Traps e informa	Traps e informa
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	Usuário USM para cada destino de trap

Limitações

- StorageGRID suporta acesso MIB somente leitura. Acesso de leitura e gravação não é suportado.
- Todos os nós da grade recebem a mesma configuração.
- SNMPv3: StorageGRID não suporta o Modo de Suporte de Transporte (TSM).
- SNMPv3: o único protocolo de autenticação suportado é o SHA (HMAC-SHA-96).
- SNMPv3: o único protocolo de privacidade suportado é o AES.

Configure o agente SNMP no StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Sobre esta tarefa

O agente SNMP do StorageGRID é compatível com SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, somente a autenticação User Security Model (USM) é suportada.

Todos os nós da grade utilizam a mesma configuração SNMP.

Especifique a configuração básica

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

Passos

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

   A página do agente SNMP é exibida.

2. Para ativar o agente SNMP em todos os nós da grid, selecione a caixa de seleção **Enable SNMP**.
3. Insira as seguintes informações na seção de configuração básica.

Campo	Descrição
Contato do sistema	Opcional. O contato principal para o sistema StorageGRID, que é retornado em mensagens SNMP como sysContact. O contato do sistema é normalmente um endereço de e-mail. Esse valor se aplica a todos os nós do sistema StorageGRID. O **contato do sistema** pode ter no máximo 255 caracteres.
Localização do sistema	Opcional. A localização do sistema StorageGRID, que é retornada nas mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde seu sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. Esse valor se aplica a todos os nós do sistema StorageGRID. **Localização do sistema** pode ter no máximo 255 caracteres.
Ativar notificações do agente SNMP	• Se selecionado, o agente SNMP do StorageGRID envia notificações de trap e inform. • Caso não seja selecionada, o agente SNMP permite acesso somente leitura ao MIB, mas não envia notificações SNMP.
Habilitar armadilhas de autenticação	Se selecionado, o agente SNMP do StorageGRID envia traps de autenticação se receber mensagens de protocolo com autenticação incorreta.

Insira as strings da comunidade

Se você utiliza SNMPv1 ou SNMPv2c, preencha a seção "Cadeias de comunidade".

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

Passos

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

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

   Cada sequência de comunidade pode ter no máximo 32 caracteres e não pode conter caracteres de

espaço em branco.

2. Selecione **Adicionar outra string de comunidade** para adicionar strings adicionais.

   São permitidas até cinco strings.

Criar destinos de trap

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

Passos

1. No campo **Comunidade de traps padrão**, insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de traps SNMPv1 ou SNMPv2.

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

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

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

SNMPv1

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

Campo	Descrição
Tipo	Deve ser Trap para SNMPv1.
Host	Um endereço IPv4 ou IPv6 ou um nome de domínio totalmente qualificado (FQDN) para receber o trap.
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 trap SNMP, a menos que você precise usar TCP.
String comunitária	Use a comunidade de captura padrão, se uma tiver sido especificada, ou insira uma string de comunidade personalizada para este destino de captura. A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv2c

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

Campo	Descrição
Tipo	Se o destino será usado para traps ou informs.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber o trap.
Porta	Use a porta 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 trap SNMP, a menos que você precise usar TCP.
String comunitária	Use a comunidade de captura padrão, se uma tiver sido especificada, ou insira uma string de comunidade personalizada para este destino de captura. A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv3

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

Campo	Descrição
Tipo	Se o destino será usado para traps ou informs.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber o trap.
Porta	Use a porta 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 trap SNMP, a menos que você precise usar TCP.
Usuário USM	O usuário USM que será usado para autenticação. • Se você selecionou **Trap**, somente os usuários do USM sem IDs de mecanismo autorizados serão exibidos. • Se você selecionou **Inform**, somente os usuários do USM com IDs de mecanismo autorizados são exibidos. • Se nenhum usuário for exibido: i. Crie e salve o destino do trap. ii. Acesse Criar usuários USM e crie o usuário. iii. Retorne à aba Destinos da armadilha, selecione o destino salvo na tabela e selecione **Editar**. iv. Selecione o usuário.

5. Selecione **Create**.

   O destino de trap é criado e adicionado à tabela.

Criar endereços de agente

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

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

Passos

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

Campo	Descrição
Protocolo de Internet	Se este endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se este endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Em qual rede StorageGRID o agente ficará escutando. • Redes Grid, Admin e Client: o agente SNMP ficará à escuta de consultas em todas as três redes. • Rede de grid • Rede de administração • Rede de cliente **Nota**: Se você usar a Rede do Cliente para dados não seguros 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 em que o agente SNMP deve escutar. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Nota**: Ao salvar o agente SNMP, StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que quaisquer firewalls externos permitam o acesso a essas portas.

3. Selecione **Create**.

   O endereço do agente é criado e adicionado à tabela.

Criar usuários USM

Se você estiver usando o SNMPv3, utilize a guia "Usuários USM" na seção "Outras configurações" para definir os usuários USM autorizados a consultar o MIB ou a receber traps e informs.

> Para destinos SNMPv3 *trap*, recomenda-se que você crie um usuário USM para cada Admin Node. Se cada Admin Node não tiver um usuário USM, seu sistema de gerenciamento pode parar de receber notificações se o Admin Node primário ficar inativo.

> Os destinos SNMPv3 *inform* devem ter usuários com IDs de mecanismo. Destinos SNMPv3 *trap* não podem ter usuários com IDs de mecanismo.

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

Passos

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

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

3. Selecione **Create**.

   O usuário USM é criado e adicionado à tabela.

4. Após concluir a configuração do agente SNMP, selecione **Save**.

   A nova configuração do agente SNMP entra em vigor.

Atualize o agente SNMP do StorageGRID

Você pode desativar as notificações SNMP, atualizar as strings da comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de trap.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Sobre esta tarefa

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

Passos

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

   A página do agente SNMP é exibida.

2. Para desativar o agente SNMP em todos os nós da grade, desmarque a caixa de seleção **Enable 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 a **localização do sistema**.
   b. Opcionalmente, selecione ou desmarque a caixa de seleção **Ativar notificações do agente SNMP** para controlar se o agente SNMP do StorageGRID envia notificações de trap e inform.

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

   c. Opcionalmente, selecione 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 usa SNMPv1 ou SNMPv2c, opcionalmente atualize ou adicione uma **Comunidade somente leitura** na seção Cadeias de comunidade.
5. Para atualizar os destinos das armadilhas, selecione a guia Destinos das armadilhas na seção Outras configurações.

   Use esta aba para definir um ou mais destinos para notificações de trap ou inform do StorageGRID. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

   Para obter detalhes sobre o que inserir, consulte "Criar destinos de trap".

   - Opcionalmente, atualize ou remova a comunidade de trap padrão.

Se você remover a comunidade de trap padrão, primeiro deverá garantir que todos os destinos de trap existentes usem uma string de comunidade personalizada.

- Para adicionar um destino de trap, selecione **Criar**.
- Para editar um destino de trap, selecione o botão de opção e selecione **Editar**.
- Para remover um destino de trap, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

6. Para atualizar os endereços dos agentes, selecione a guia Endereços dos agentes na seção Outras configurações.

   Use esta aba 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 inserir, consulte "Criar endereços de agente".

   - Para adicionar um endereço de agente, selecione **Criar**.
   - Para editar o endereço de um agente, selecione o botão de opção e selecione **Editar**.
   - Para remover o endereço de um agente, selecione o botão de opção e selecione **Remover**.
   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

7. Para atualizar os usuários do USM, selecione a guia "Usuários do USM" na seção "Outras configurações".

   Use esta aba para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber traps e informs.

   Para obter detalhes sobre o que inserir, consulte "Criar usuários USM".

   - Para adicionar um usuário USM, selecione **Criar**.
   - Para editar um usuário do USM, selecione o botão de opção e selecione **Editar**.

     O nome de usuário de um usuário USM existente não pode ser alterado. Se você precisar alterar um nome de usuário, deve remover o usuário e criar um novo.

     > Se você adicionar ou remover o ID do mecanismo autorizado de um usuário e esse usuário estiver selecionado para um destino, você deve editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

   - Para remover um usuário do USM, selecione o botão de opção e selecione **Remover**.

     > Se o usuário que você removeu estiver selecionado para um destino de trap, você deve editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando você atualizar a configuração do agente SNMP, selecione **Salvar**.

Acesse os arquivos MIB do StorageGRID

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e serviços gerenciados para os nós da sua grid. Você pode acessar os arquivos MIB que

definem os objetos e notificações para StorageGRID. Esses arquivos podem ser úteis para monitorar sua grid.

Consulte "Use o monitoramento SNMP" para obter mais informações sobre SNMP e arquivos MIB.

Acesse os arquivos MIB

Siga estes passos para acessar os arquivos MIB.

Passos

1. Selecione **Configuração** > **Monitoramento** > **Agente SNMP**.
2. Na página do agente SNMP, selecione o arquivo que você deseja baixar:
   - **NETAPP-STORAGEGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os Admin Nodes.
   - **ES-NETAPP-06-MIB.mib**: Define objetos e notificações para appliances baseados em E-Series.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com interface BMC.

   Você também pode acessar os arquivos MIB no seguinte local em qualquer nó do StorageGRID: `/usr/share/snmp/mibs`

3. Para extrair os OIDs do StorageGRID do arquivo MIB:
   a. Obtenha o OID da raiz do StorageGRID MIB:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Resultado: `.1.3.6.1.4.1.789.28669` (`28669` é sempre o OID para StorageGRID)

   b. Procure o OID do StorageGRID em toda a árvore (usando `paste` para unir linhas):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

   O `snmptranslate`comando possui diversas opções úteis para explorar o MIB. Este comando está disponível em qualquer nó do StorageGRID.

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID do StorageGRID.

Nome do objeto	ID do objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID.

Objetos MIB

Nome do objeto	ID do objeto (OID)	Tipo	Acesso	Módulo MIB	Descrição
activeAlertCount		Integer32	Somente leitura	NETAPP-STORAGEGRID-MIB	O número de alertas ativos na activeAlertTable.
activeAlertTable		Sequência de ActiveAlertEntry	Não acessível	NETAPP-STORAGEGRID-MIB	Uma tabela de alertas ativos no StorageGRID.
activeAlertEntry		Sequência	Não acessível	NETAPP-STORAGEGRID-MIB	Um único alerta do StorageGRID, indexado pelo ID do alerta.
activeAlertId		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
activeAlertName		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O nome do alerta.
activeAlertInstance		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O nome da entidade que gerou o alerta, normalmente o nome do nó.
activeAlertSeverity		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	A gravidade do alerta.
activeAlertStartTime		Data e hora	Somente leitura	NETAPP-STORAGEGRID-MIB	O horário em que o alerta foi acionado.

Coletar dados adicionais do StorageGRID

Monitore o desempenho das operações PUT e GET no StorageGRID

Você pode monitorar o desempenho de determinadas operações, como armazenamento de objetos e recuperação, para ajudar a identificar alterações que possam exigir uma investigação mais aprofundada.

Sobre esta tarefa

Para monitorar o desempenho das operações PUT e GET, você pode executar comandos S3 diretamente de uma estação de trabalho ou usando o aplicativo de código aberto S3tester. Usar esses métodos permite que você avalie o desempenho independentemente de fatores externos ao StorageGRID, como problemas com um aplicativo cliente ou com uma rede externa.

Ao realizar testes de operações PUT e GET, utilize as seguintes diretrizes:

- Use tamanhos de objeto comparáveis aos objetos que você normalmente ingere em seu grid.
- Execute operações em sites locais e remotos.

As mensagens no "log de auditoria" indicam o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação S3 GET, você pode consultar o valor do atributo TIME na mensagem de log de auditoria SGET. Você também pode encontrar o atributo TIME nas mensagens de log de auditoria para as seguintes operações S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como a produtividade geral que você consegue alcançar. Repita os mesmos testes regularmente e registre os resultados, para que você possa identificar tendências que possam exigir investigação.

- Você pode "Baixe o S3tester do github".

Monitor operações de verificação de objetos no StorageGRID

O sistema StorageGRID pode verificar a integridade dos dados dos objetos nos nós de armazenamento, verificando tanto objetos corrompidos quanto ausentes.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso de manutenção ou root".

Sobre esta tarefa

Dois "processos de verificação" trabalham juntos para garantir a integridade de 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 Storage Nodes para determinar se existem cópias corrompidas de dados de objetos replicados e codificados por eliminação. Se forem encontrados problemas, o sistema StorageGRID tenta automaticamente substituir os dados de objetos corrompidos por cópias armazenadas em outro local do sistema. A verificação em segundo plano não é executada em objetos em um Cloud Storage Pool.

  > ⓘ O alerta **Objeto corrompido não identificado detectado** é acionado se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente.

- A **verificação de existência de objeto** pode ser acionada por você para verificar mais rapidamente a existência (embora não a exatidão) dos dados do objeto.

  A verificação de existência de objetos verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados para apagamento existem em um Storage Node. A verificação de existência de objetos fornece uma maneira de verificar a integridade dos dispositivos de storage, especialmente se um problema recente de hardware puder ter afetado a integridade de dados.

Você deve revisar regularmente os resultados das verificações em segundo plano e das verificações de existência de objetos. Investigue imediatamente quaisquer casos de dados de objetos corrompidos ou ausentes para determinar a causa raiz.

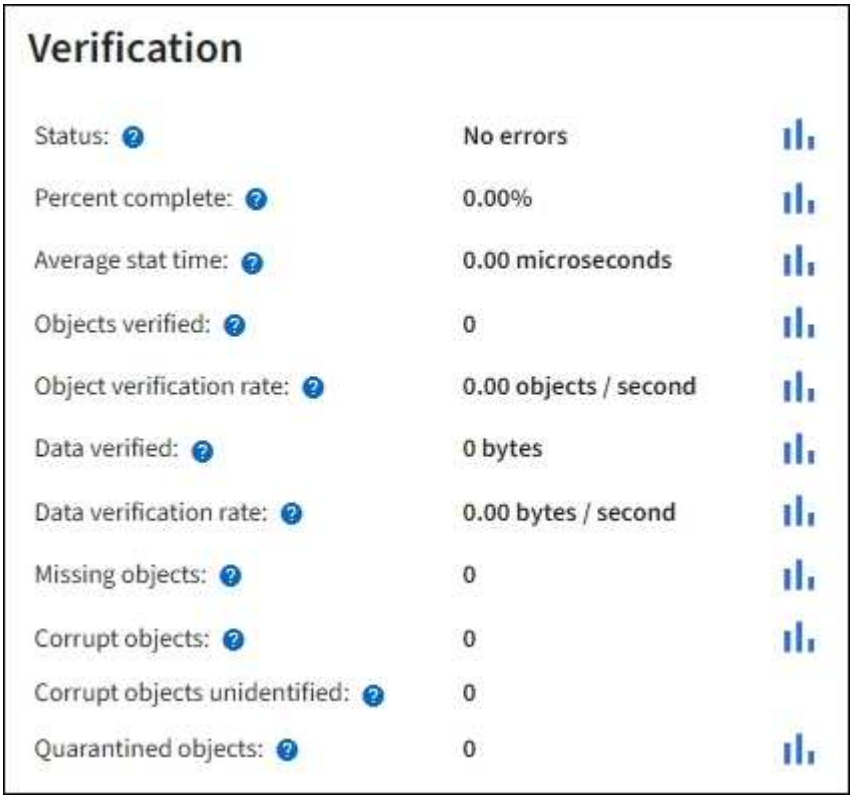
Passos

1. Analise os resultados das verificações de antecedentes:

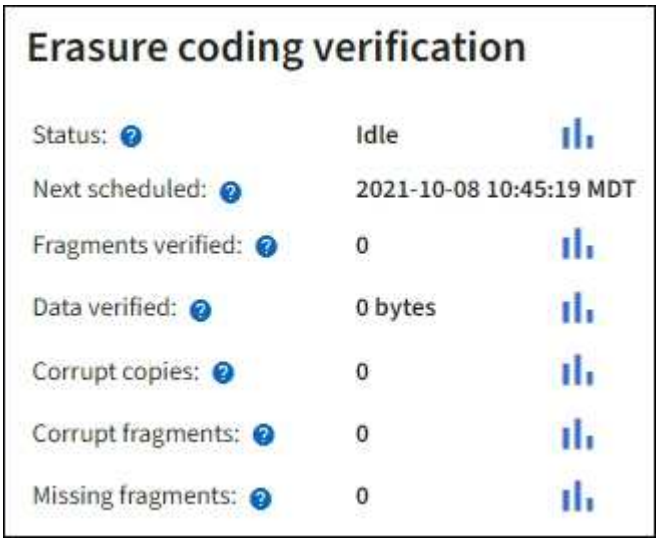
   a. Selecione **Nodes** > ***Storage Node*** > **Objects**.

   b. Confira os resultados da verificação:

      - Para verificar a autenticação dos dados do objeto replicado, consulte os atributos na seção Verificação.

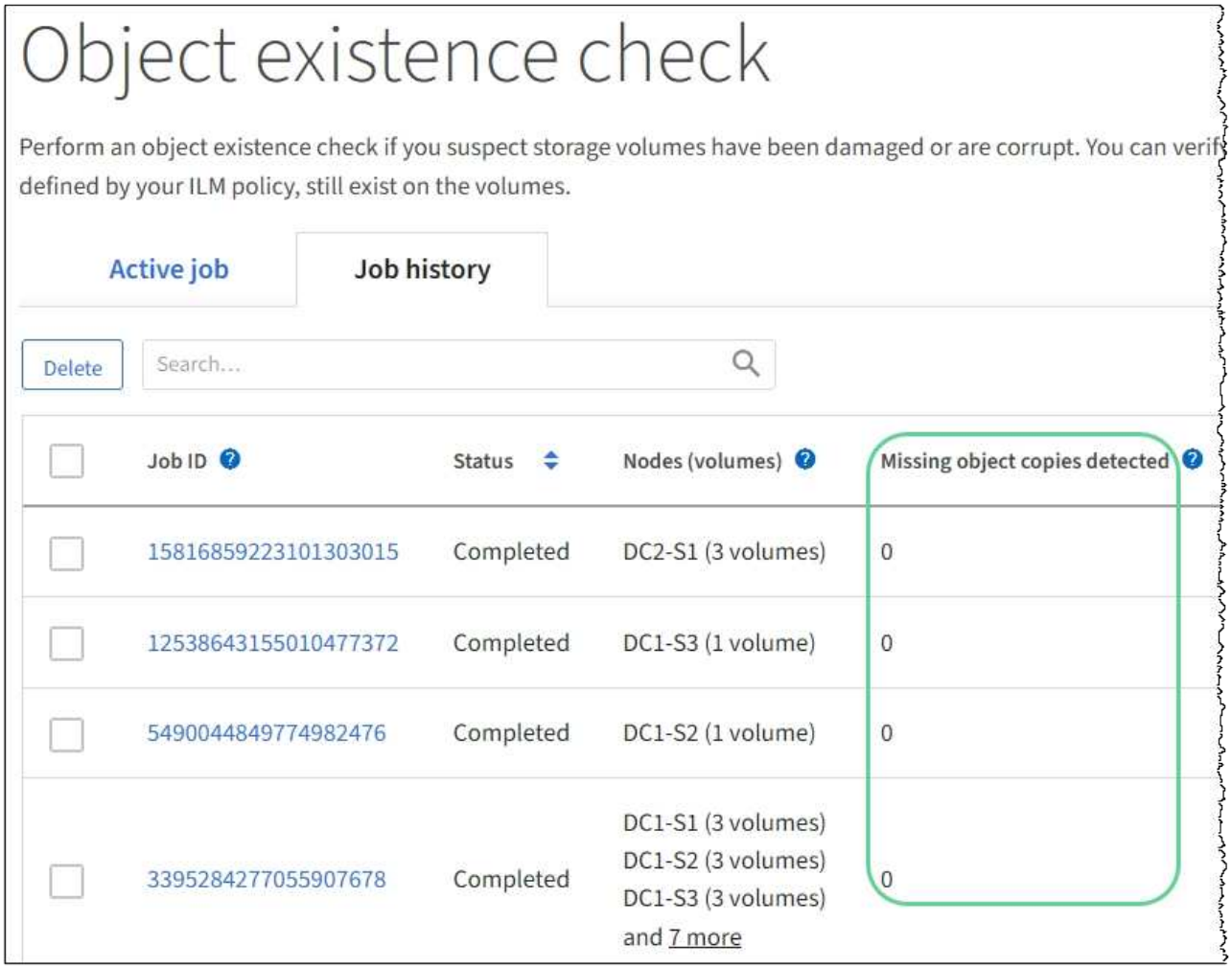


      - Para verificar a verificação de fragmentos codificados por apagamento, selecione ***Storage Node*** > **ILM** e observe os atributos na seção Verificação de codificação de apagamento.



   Selecione o ponto de interrogação (?) ao lado do nome de um atributo para exibir o texto de ajuda.

2. Analise os resultados das tarefas de verificação de existência de objetos:
   a. Selecione **Manutenção** > **Verificação de existência do objeto** > **Histórico de tarefas**.
   b. Analise a coluna "Cópias de objetos ausentes detectadas". Se alguma tarefa resultar em 100 ou mais cópias de objetos ausentes e o alerta "Objetos potencialmente perdidos" for acionado, entre em contato com o suporte técnico.



Analise as mensagens de auditoria do StorageGRID

As mensagens de auditoria podem ajudar você a entender melhor o funcionamento detalhado do seu sistema StorageGRID. Você pode usar os logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços do StorageGRID geram mensagens de auditoria, conforme descrito a seguir:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos dentro do StorageGRID, incluindo storage de objetos e recuperações, transferências de nó da grade para nó da grade e verificações.
- As mensagens de log de auditoria de leitura e gravação do cliente são registradas quando um aplicativo

cliente S3 faz uma solicitação para criar, modificar ou recuperar um objeto.

- As mensagens de auditoria de gerenciamento registram as solicitações do usuário para a Management API.

Cada nó administrativo armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log) assim como logs de auditoria compactados de dias anteriores. Cada nó na grid também armazena uma cópia das informações de auditoria geradas no nó.

Você pode acessar os arquivos de log de auditoria diretamente da linha de comando do Nó de Administração.

StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- StorageGRID utiliza, por padrão, destinos de log de auditoria de nós locais.
- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de armazenamento.
- Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar as informações de auditoria para um servidor syslog externo. Os logs locais de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo está configurado.
- "Saiba mais sobre como configurar o gerenciamento de logs".

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 as mensagens de auditoria, consulte "Analisar registros de auditoria".

Coletar arquivos de log do StorageGRID e dados do sistema

Você pode recuperar arquivos de log do StorageGRID e dados do sistema, incluindo dados de configuração, e enviá-los para o suporte técnico.

Antes de começar

- Você está conectado ao Gerenciador de Grade em qualquer Nó de Administração usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você possui a senha de provisionamento.

Sobre esta tarefa

Utilize o Grid Manager para coletar "arquivos de log"dados do sistema e dados de configuração de qualquer nó da grid durante o período que você selecionar. Os dados são coletados e arquivados em um `.tar.gz` arquivo que você pode então baixar para o seu computador local ou enviar para o suporte técnico.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais de registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo está configurado. Consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

Passos

1. Selecione **Suporte** > **Ferramentas** > **Coleta de logs**. Uma tabela de nós é exibida.
2. Selecione os nós da grade para os quais você deseja coletar arquivos de log.

   Você pode classificar por nome do nó, site e tipo de nó. As colunas Site e Tipo de nó contêm filtros para selecionar sites e tipos de nó individuais.

3. Selecione **Continue**.
4. Selecione o intervalo de data e hora dos dados a serem incluídos nos arquivos de log.

   Se você selecionar um período muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de logs poderá ficar grande demais para ser armazenado em um nó ou grande demais para ser coletado por um nó de administração para download. Se algum desses cenários ocorrer, reinicie a coleta de logs com um conjunto de dados menor.

5. Selecione os tipos de logs que você deseja coletar.
   - **Logs de aplicativos**: Logs específicos do aplicativo que o suporte técnico usa com mais frequência para solucionar problemas. Os logs coletados são um subconjunto dos logs de aplicativos disponíveis.
   - **Registros de auditoria**: Registros contendo as mensagens de auditoria geradas durante a operação normal do sistema.
   - **Rastreamento de rede**: logs usados para depuração de rede.
   - **Banco de dados Prometheus**: métricas de séries temporais dos serviços em todos os nós.
6. Opcionalmente, utilize a caixa de texto **Notas** para inserir anotações sobre os arquivos de log que você está coletando.

   Você pode usar essas anotações para fornecer informações de suporte técnico sobre o problema que levou você a coletar os arquivos de log. Suas anotações são adicionadas a um arquivo chamado `info.txt`, juntamente com outras informações sobre a coleta dos arquivos de log. O arquivo `info.txt` é salvo no pacote de arquivamento de arquivos de log.

7. Na caixa de texto **Senha de provisionamento**, insira a senha de provisionamento do seu sistema StorageGRID.
8. Selecione **Coletar logs**.

   Você pode usar a página de coleta de logs para monitorar o progresso da coleta de arquivo de log para cada nó da grade.

   Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo mais curto ou para um número menor de nós.

9. Se a coleta de logs falhar:
   - Se a mensagem "Falha na coleta de logs" for exibida, você pode tentar coletar os logs novamente ou encerrar a sessão sem tentar novamente.
   - Se a mensagem "Coleta de logs falhou parcialmente" for exibida, você pode tentar coletar os logs novamente, encerrar a sessão, baixar o arquivo de log ou enviar o arquivo de log para AutoSupport.
10. Quando a coleta do arquivo de log estiver concluída:
    - Selecione **Download** para baixar o arquivo `.tar.gz`.
    - Selecione **Enviar para AutoSupport** para enviar o `.tar.gz` arquivo para suporte técnico.

      O `.tar.gz`arquivo contém todos os arquivos de log de todos os nós da grade onde a coleta de logs foi bem-sucedida. O `.tar.gz`arquivo combinado contém um arquivo de log para cada nó da grade.

    O assunto do pacote AutoSupport é `USER_TRIGGERED_SUPPORT_BUNDLE`.

11. Selecione **Concluir**.

O `.tar.gz`arquivo é excluído quando você seleciona **Concluir**. Certifique-se de baixar ou enviar o arquivo primeiro.

Acionar manualmente um pacote AutoSupport do StorageGRID

Para ajudar o suporte técnico a solucionar problemas com seu sistema StorageGRID, você pode acionar manualmente o envio de um pacote AutoSupport.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você possui acesso de root ou permissão de configuração de outra grid.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport**.
2. Na aba **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   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 **Última Vez Bem-Sucedida** na aba **Resultados** são atualizados. Se houver um problema, o valor **Resultado Mais Recente** é atualizado para "Falha" e o StorageGRID não tenta enviar o pacote AutoSupport novamente.

3. Após 1 minuto, atualize a página AutoSupport no seu navegador para acessar os resultados mais recentes.

Além disso, você pode "coletar arquivos de log e dados do sistema mais extensos" e enviá-los para o site de suporte da NetApp.

Analisar métricas de suporte do StorageGRID

Ao solucionar um problema, você pode trabalhar com o suporte técnico para revisar métricas e gráficos detalhados do seu sistema StorageGRID.

Antes de começar

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

Sobre esta tarefa

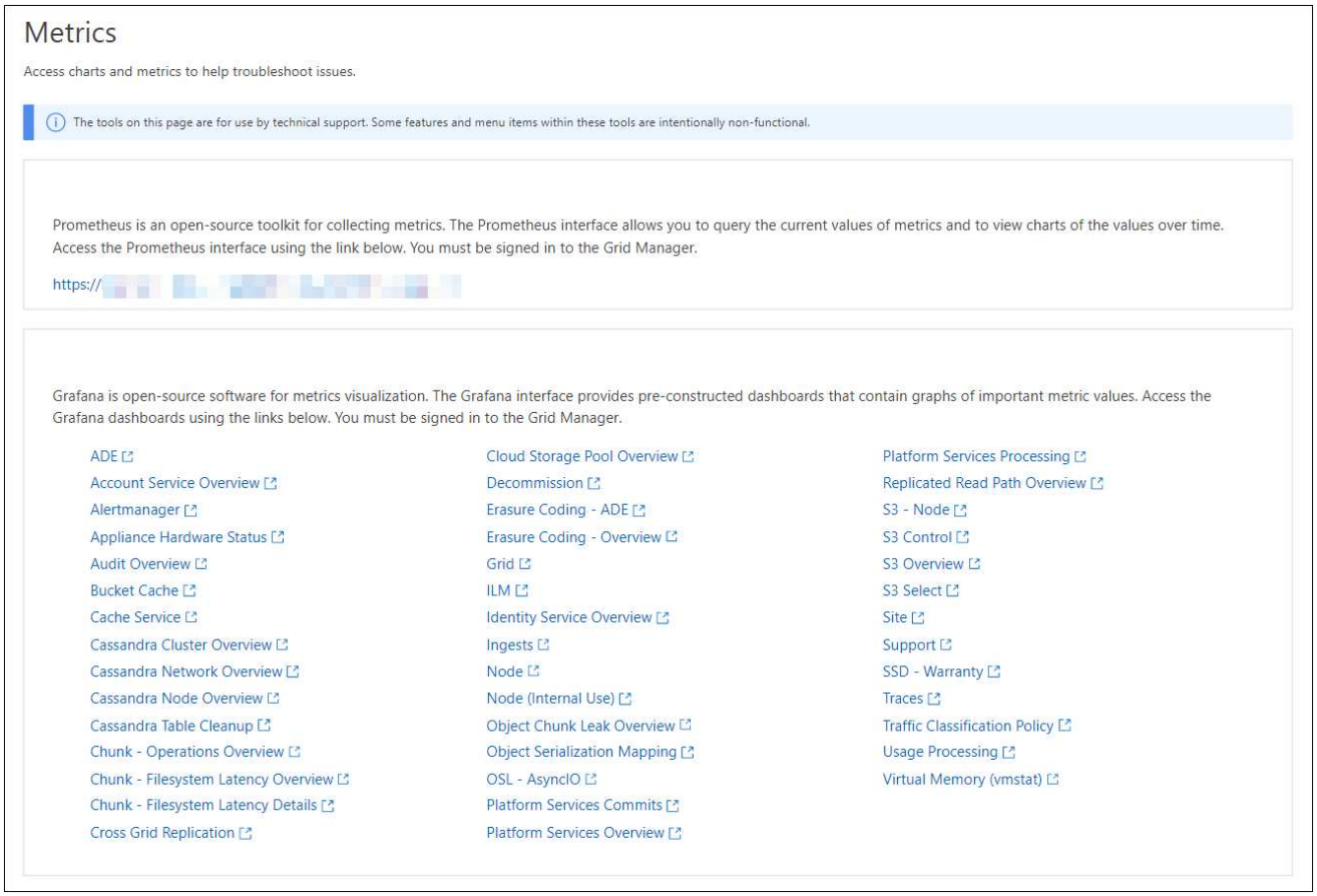
A página Métricas permite que você acesse as interfaces de usuário do Prometheus e do Grafana. Prometheus é um software de código aberto para coleta de métricas. Grafana é um software de código aberto para visualização de métricas.

As ferramentas disponíveis na página Métricas destinam-se ao uso pelo suporte técnico. Alguns recursos e itens de menu nessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Consulte a lista de "métricas Prometheus comumente usadas".

Passos

1. Conforme orientação do suporte técnico, selecione **Support** > **Tools** > **Metrics**.

   Um exemplo da página de Métricas é mostrado aqui:



2. Para consultar os valores atuais das métricas do StorageGRID e visualizar gráficos desses valores ao longo do tempo, clique no link na seção Prometheus.

   A interface Prometheus é exibida. Você pode usar essa interface para executar consultas nas métricas do StorageGRID e para gerar gráficos das métricas do StorageGRID ao longo do tempo.

   > As métricas que incluem *private* em seus nomes destinam-se apenas ao uso interno e estão sujeitas a alterações entre versões do StorageGRID sem aviso prévio.

3. Para acessar painéis pré-construídos contendo gráficos das métricas do StorageGRID ao longo do tempo, clique nos links na seção Grafana.

   A interface do Grafana para o link que você selecionou é exibida.

Alterar a priorização de E/S no StorageGRID

A priorização de entrada/saída (E/S) permite que você altere as prioridades relativas das operações de E/S na grid.

Por padrão, o tráfego de E/S PUT e GET do cliente recebe a maior prioridade em relação a atividades em segundo plano, como a limpeza de dados codificados por apagamento (EC) e o reparo de EC. Ao aumentar a prioridade das atividades de limpeza de dados codificados por apagamento (EC) e reparo de EC, essas tarefas podem ser concluídas mais rapidamente. A eficácia das alterações na priorização de E/S é impactada pela taxa de solicitações do cliente, flutuações no tráfego de rede e outras tarefas de rede em andamento.

Antes de começar

- Analise a página de priorização de E/S para determinar quais opções podem afetar sua grid.
- Avalie se o tráfego de clientes em andamento pode lidar com segurança com tempos de espera mais longos ou timeouts do cliente.
- Esteja preparado para monitorar o efeito da mudança de priorização e ajustar conforme necessário. Essas mudanças são implementadas rapidamente, mas seu efeito pode levar horas para se tornar visível.

Passos

1. Selecione **Support** > **I/O prioritization**.
2. (Opcional) Altere a prioridade de limpeza e reparo do EC para operações em segundo plano que excluem dados do EC, de seus valores padrão.

   Use a prioridade padrão baixa de limpeza e reparo de EC para grids que têm nós baseados em RAID.

3. Selecione **Salvar**.
4. Monitore "métricas" para avaliar o efeito das mudanças de priorização.

Execute diagnósticos no StorageGRID

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos em seu sistema StorageGRID e analisar os resultados.

- "Análise das métricas de suporte"
- "Métricas Prometheus comumente usadas"

Antes de começar

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

Sobre esta tarefa

A página Diagnóstico executa um conjunto de verificações de diagnóstico no estado atual da grid. Cada verificação de diagnóstico pode ter um dos três status:

- **Normal**: Todos os valores estão dentro da faixa normal.
- **Atenção**: Um ou mais valores estão fora da faixa normal.
- **Atenção**: Um ou mais valores estão significativamente fora da faixa normal.

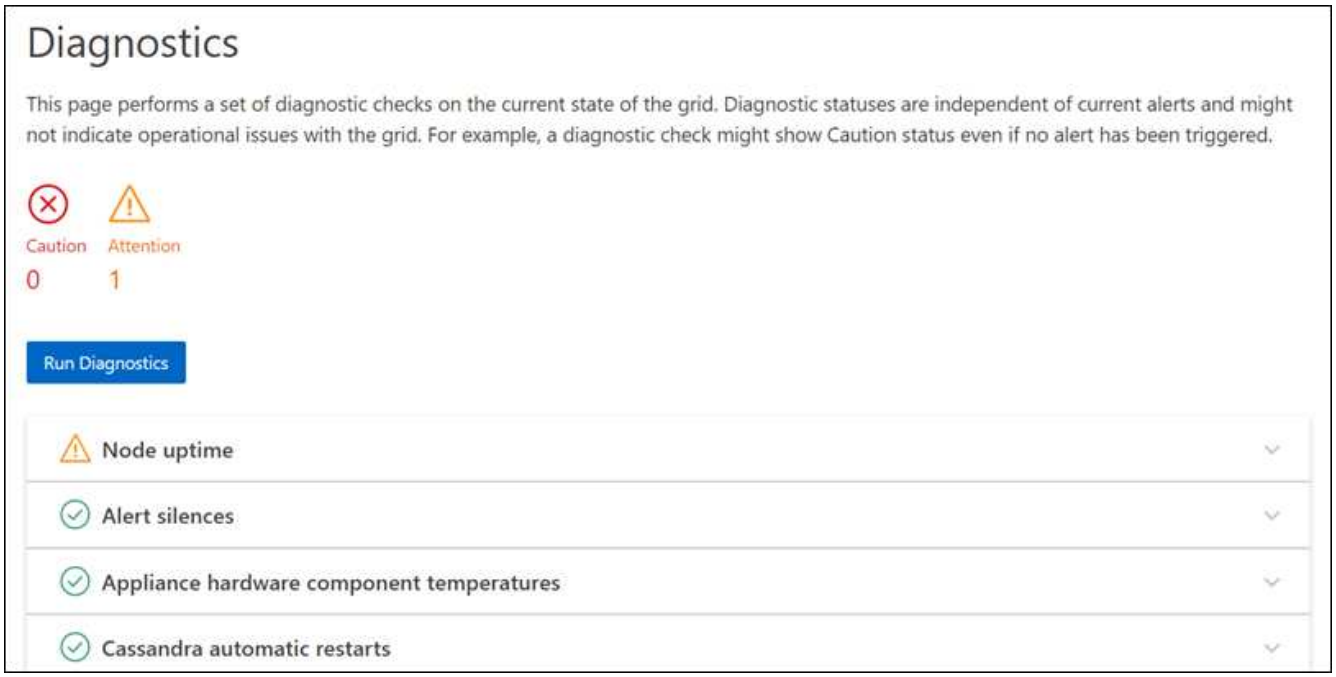
Os status de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais na grid. Por exemplo, uma verificação de diagnóstico pode mostrar o status de Atenção mesmo que nenhum alerta tenha sido acionado.

Passos

1. Selecione **Suporte** > **Ferramentas** > **Diagnóstico**.

   A página de Diagnóstico é exibida e lista os resultados de cada verificação diagnóstica. Os resultados são classificados por gravidade (Cuidado, Atenção e, em seguida, Normal). Dentro de cada nível de gravidade, os resultados são classificados em ordem alfabética.

   Neste exemplo, um diagnóstico tem o status de Atenção e três diagnósticos têm o status de Normal.



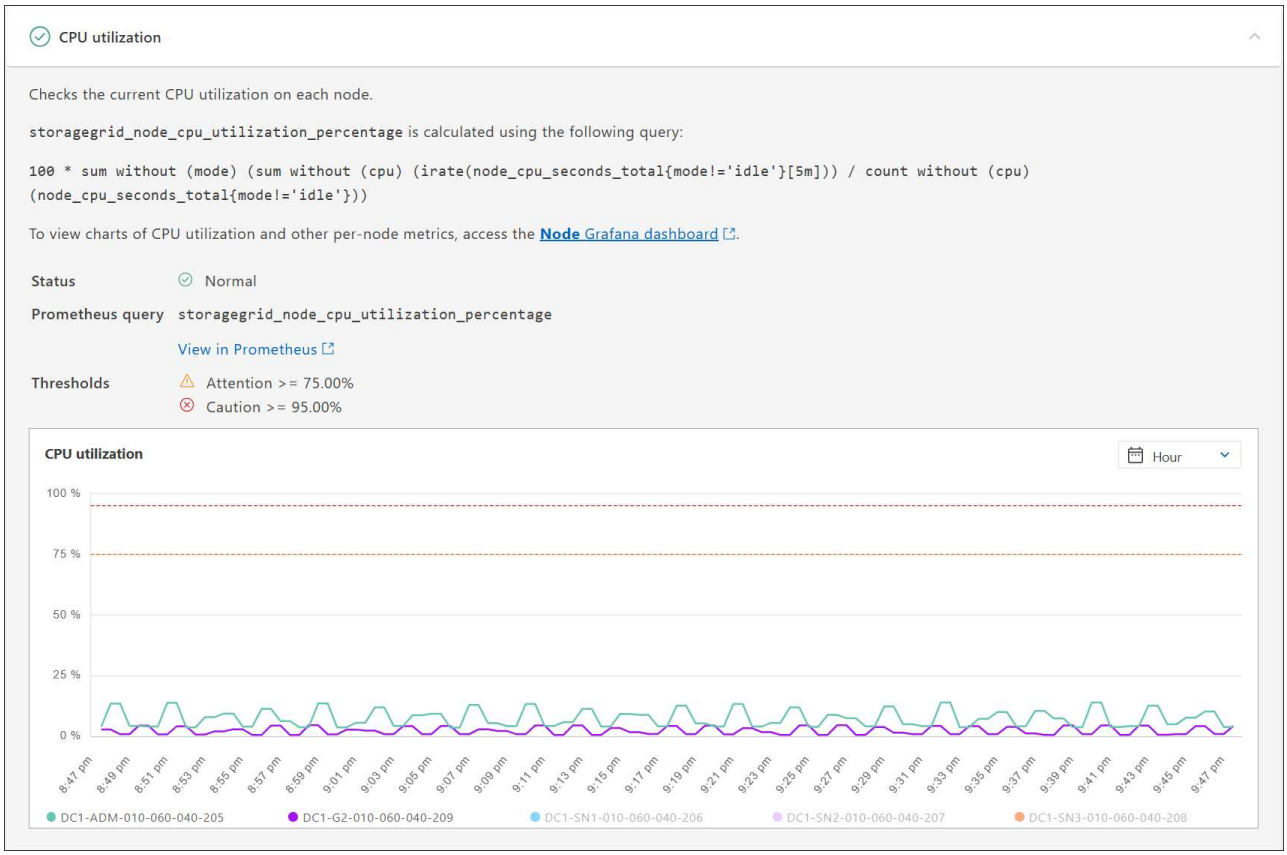
2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

   Detalhes sobre o diagnóstico e seus resultados atuais são exibidos. Os seguintes detalhes são listados:

   - **Status**: O status 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 status diagnóstico anormal. (Os valores de limiar não são usados para todos os diagnósticos.)

     Você não pode alterar esses limites.

   - **Valores de status**: Um gráfico e uma tabela (tabela não mostrada na captura de tela) mostram o status e o valor do diagnóstico em todo o sistema StorageGRID. Neste exemplo, é mostrada a utilização de CPU atual para cada nó em um sistema StorageGRID. Todos os valores dos nós estão abaixo dos limites de Atenção e Cuidado, então o status geral do diagnóstico é Normal.



3. **Opcional**: Para visualizar os gráficos do Grafana relacionados a este diagnóstico, selecione **Grafana dashboard**.

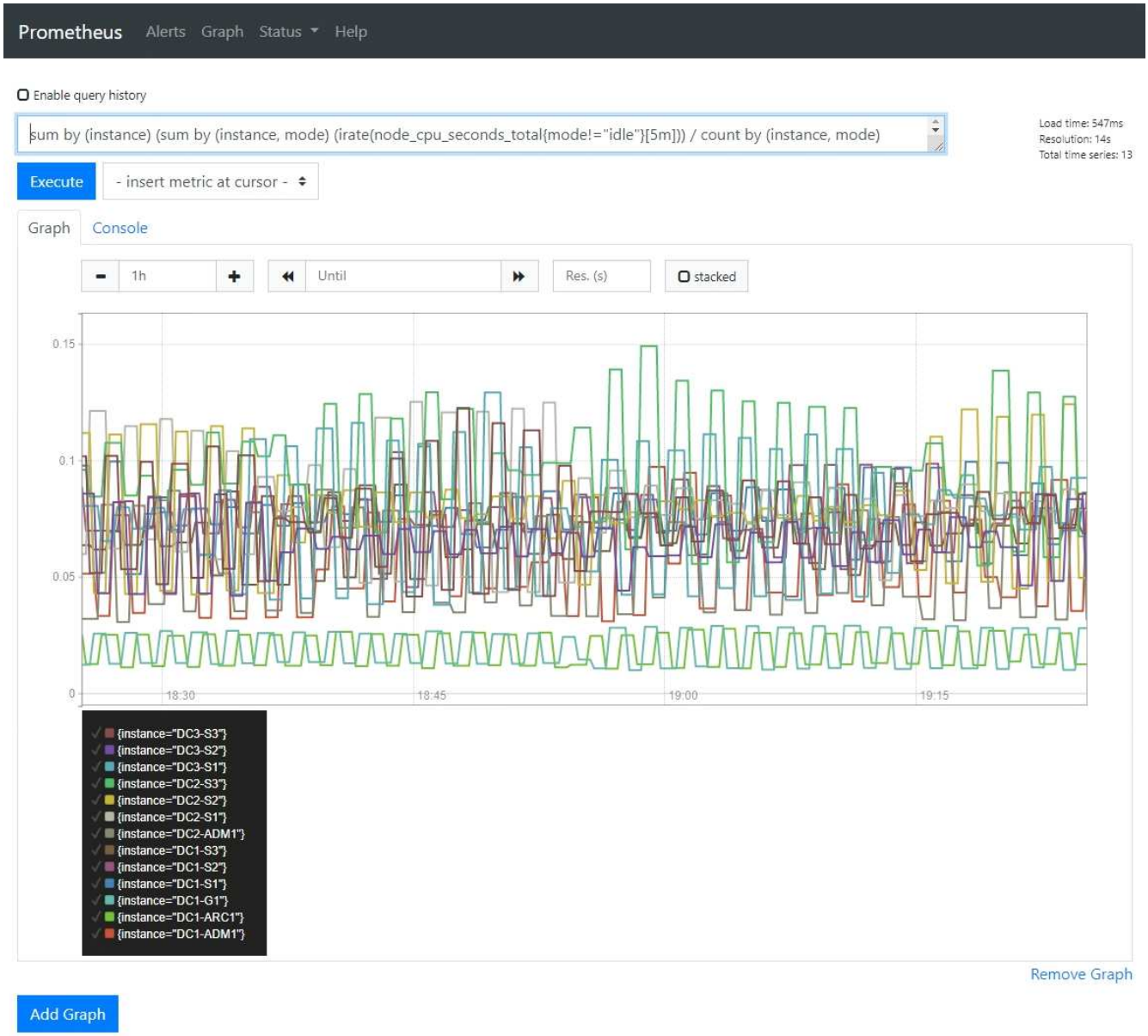
   Este link não é exibido para todos os diagnósticos.

   O painel do Grafana correspondente é exibido. Neste exemplo, o painel do nó é exibido mostrando a utilização de CPU ao longo do tempo para este nó, assim como outros gráficos do Grafana para o nó.

   > Você também pode acessar os painéis pré-construídos do Grafana na seção Grafana da página **Suporte** > **Ferramentas** > **Métricas**.

4. **Opcional**: Para ver um gráfico da expressão Prometheus ao longo do tempo, clique em **Ver no Prometheus**.

   Aparece um gráfico Prometheus da expressão utilizada no diagnóstico.



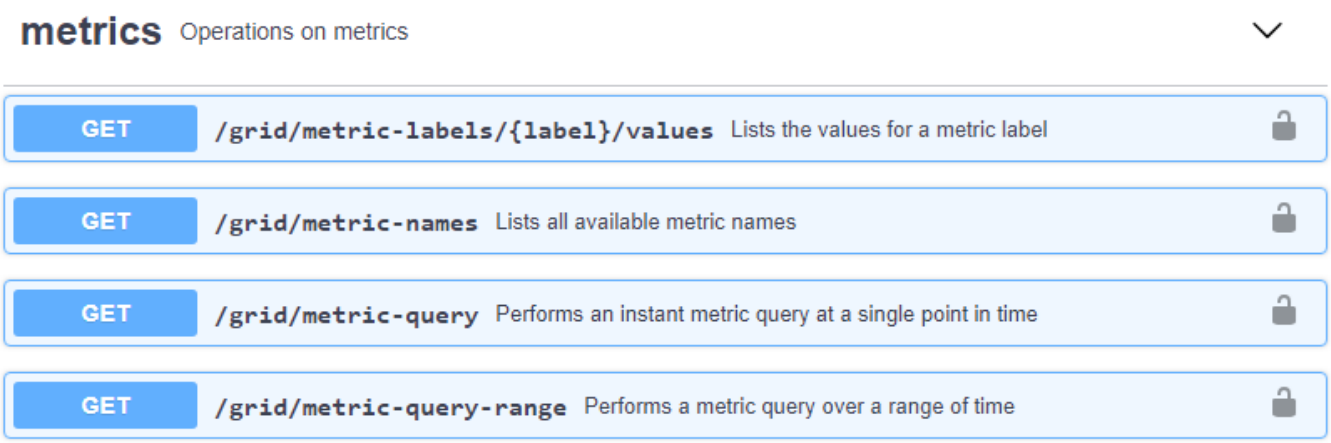
Crie aplicativos de monitoramento personalizados para StorageGRID

Você pode criar aplicativos e painéis de monitoramento personalizados usando as métricas do StorageGRID disponíveis na API de Gerenciamento de Grid.

Se você deseja monitorar métricas que não são exibidas em uma página existente do Grid Manager, ou se deseja criar painéis personalizados para StorageGRID, você pode usar a Grid Management API para consultar métricas do StorageGRID.

Você também pode acessar as métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como o Grafana. O uso de uma ferramenta externa exige que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Consulte o "Instruções para administrar StorageGRID".

Para visualizar as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Grid Manager. Na parte superior da página, selecione o ícone de ajuda e selecione **API documentation** > **métricas**.



Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo desta documentação.

Solucione problemas do sistema StorageGRID

Solucione problemas em um sistema StorageGRID

Se você encontrar um problema ao usar um sistema StorageGRID, consulte as dicas e orientações desta seção para obter ajuda na identificação e resolução do problema.

Muitas vezes, você consegue resolver problemas sozinho; no entanto, pode ser necessário escalar algumas questões para o suporte técnico.

Defina o problema

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

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

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não fazendo? Quais são os seus sintomas?	Os aplicativos cliente estão relatando que os objetos não podem ser inseridos no StorageGRID.
Quando o problema começou?	A ingestão do objeto foi negada pela primeira vez por volta das 14:50 do dia 8 de janeiro de 2020.
Como você percebeu o problema pela primeira vez?	Notificado pelo aplicativo cliente. Também recebeu notificações de alerta por e-mail.
O problema ocorre sempre ou apenas às vezes?	O problema persiste.
Se o problema ocorre regularmente, quais etapas fazem com que ele ocorra	O problema ocorre sempre que um cliente tenta ingerir um objeto.

Pergunta	Exemplo de resposta
Se o problema ocorrer de forma intermitente, quando ele acontece? Registre os horários de cada incidente de que você tiver conhecimento.	O problema não é intermitente.
Você já se deparou com esse problema antes? Com que frequência você teve esse problema no passado?	É a primeira vez que me deparo com esse problema.

Avalie o risco e o impacto no sistema

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

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

Pergunta	Exemplo de resposta
O sistema StorageGRID consegue ingerir conteúdo?	Não
Os aplicativos cliente podem recuperar conteúdo?	Alguns objetos podem ser recuperados e outros não.
Os dados estão em risco?	Não
A capacidade de conduzir negócios está gravemente 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

Após definir o problema e avaliar seus riscos e impactos, colete dados para análise. O tipo de dado mais útil a ser coletado depende da natureza do problema.

Tipo de dados a serem coletados	Por que coletar esses dados	Instruções
Criar linha do tempo das mudanças recentes	Alterações no seu sistema StorageGRID, na sua configuração ou no seu ambiente podem causar novos comportamentos.	• Crie uma linha do tempo das mudanças recentes

Tipo de dados a serem coletados	Por que coletar esses dados	Instruções
Revisar alertas	Os alertas podem ajudar você a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre as questões subjacentes que podem estar causando isso. Consulte a lista de alertas atuais para verificar se StorageGRID identificou a causa raiz de um problema para você. Analise os alertas acionados no passado para obter informações adicionais.	• "Veja os alertas atuais e resolvidos"
Estabeleça linhas de base	Reúna informações sobre os níveis normais de vários valores operacionais. Esses valores de referência e os desvios em relação a eles podem fornecer pistas valiosas.	• Estabeleça linhas de base
Realize testes de ingestão e recuperação	Para solucionar problemas de desempenho com a ingestão e recuperação de dados, utilize uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com aqueles obtidos ao usar o aplicativo cliente.	• "Monitore o desempenho de PUT e GET"
Revisar mensagens de auditoria	Analise as mensagens de auditoria para acompanhar em detalhes as operações do StorageGRID. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Revisar mensagens de auditoria"
Verifique a localização dos objetos e a integridade do armazenamento	Se estiver com problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados dos objetos em um Storage Node.	• "Monitorar operações de verificação de objetos" • "Confirme os locais dos dados do objeto" • "Verificar integridade do objeto"
Coletar dados para suporte técnico	O suporte técnico poderá solicitar que você colete dados ou revise informações específicas para ajudar na resolução de problemas.	• "Coletar arquivos de log e dados do sistema" • "Acionar manualmente um pacote AutoSupport" • "Análise das métricas de suporte"

Crie uma linha do tempo das mudanças recentes

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

- Alterações no seu sistema StorageGRID, na sua configuração ou no seu ambiente podem causar novos comportamentos.
- Uma linha do tempo das alterações pode ajudar você a identificar quais mudanças podem ser responsáveis por um problema e como cada mudança pode ter afetado seu desenvolvimento.

Crie uma tabela com as alterações recentes do seu sistema, incluindo informações sobre quando cada alteração ocorreu e quaisquer detalhes relevantes sobre a alteração, como informações sobre o que mais estava acontecendo enquanto a alteração estava em andamento:

Tempo de mudança	Tipo de alteração	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização do software foi concluída? • Você interrompeu o processo?	O que aconteceu? O que você fez?	Documente todos os detalhes relevantes sobre a alteração. Por exemplo: • Detalhes das alterações na rede. • Qual hotfix foi instalado. • Como as cargas de trabalho dos clientes mudaram. Certifique-se de observar se mais de uma alteração ocorreu simultaneamente. Por exemplo, essa alteração foi feita durante uma atualização em andamento?

Exemplos de mudanças significativas recentes

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi instalado, expandido ou recuperado recentemente?
- O sistema foi atualizado recentemente? Um hotfix foi aplicado?
- Algum componente do hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?
- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento foram alterados?
- Você alterou os balanceadores de carga ou adicionou ou removeu um grupo de alta disponibilidade de Admin Nodes ou Gateway Nodes?
- Alguma tarefa foi iniciada e pode levar muito tempo para ser concluída? Exemplos incluem:
  - Recuperação de um nó de armazenamento com falha
  - Desativação de Storage Node
- Houve alguma alteração na autenticação do usuário, como a adição de um tenant ou a alteração da configuração LDAP?
- A migração de dados está ocorrendo?

- Os serviços da plataforma foram ativados ou alterados recentemente?
- A conformidade foi ativada recentemente?
- Pools de armazenamento em nuvem foram adicionados ou removidos?
- Houve alguma alteração na compressão de armazenamento ou criptografia?
- Houve alguma alteração na infraestrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Houve alguma alteração nas fontes do NTP?
- Houve alguma alteração nas interfaces de Grid, Admin ou Cliente?
- ${post_edited_translations.segment}

Estabeleça linhas de base

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

Propriedade	Valor	Como obter
Consumo médio de armazenamento	GB consumidos/dia Percentual consumido por dia	Acesse o Grid Manager. Na página Nodes, selecione toda a grid ou um site e acesse a guia Storage. No gráfico "Armazenamento Utilizado - Dados do Objeto", encontre um período em que a linha esteja relativamente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.
Consumo médio de metadados	GB consumidos/dia Percentual consumido por dia	Acesse o Grid Manager. Na página Nodes, selecione toda a grid ou um site e acesse a guia Storage. No gráfico "Armazenamento Utilizado - Metadados do Objeto", encontre um período em que a linha esteja relativamente 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	Operações/segundo	No painel do Grid Manager, selecione **Desempenho** > **Operações S3 para Storage Nodes**. Para visualizar as taxas e contagens de ingestão e recuperação de um site ou nó específico, selecione **Nodes** > ***site ou Storage Node*** > **Objects**. Posicione o cursor sobre o gráfico de ingestão e recuperação do S3.

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

Analisar dados

Utilize as informações que você coletar para determinar a causa do problema e possíveis soluções.

A análise depende do problema, mas, em geral:

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

Lista de verificação de informações de escalonamento

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

✔	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Ele ocorre de forma constante ou intermitente? Se intermitente, em que horários ocorreu? Defina o problema

✔	Item	Notas
	Avaliação de impacto	Qual a gravidade do problema? Qual o impacto para o aplicativo do cliente? • O cliente já se conectou com sucesso antes? • O cliente pode ingerir, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione **Manutenção** > **Sistema** > **Licença**. O ID do sistema StorageGRID é exibido como parte da licença atual.
	Versão do software	Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **About** para ver a versão do StorageGRID.
	Personalização	Resuma como seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grid utiliza compressão de armazenamento, criptografia de armazenamento ou conformidade? • O ILM cria objetos replicados ou codificados para apagamento? O ILM garante redundância entre sites? As regras do ILM usam os comportamentos de ingestão Balanced, Strict ou Dual Commit?
	Arquivos de log e dados do sistema	Colete arquivos de log e dados do sistema para seu sistema. Selecione **Support** > **Tools** > **Log collection**. Você pode coletar logs para toda a grid ou para nós selecionados. Se você estiver coletando logs apenas para nós selecionados, certifique-se de incluir pelo menos um Nó de Armazenamento que tenha o serviço ADC. Os três primeiros Nós de Armazenamento instalados em um site incluem o serviço ADC.
	Informações básicas	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabeleça linhas de base
	Cronologia das mudanças recentes	Crie uma linha do tempo que resuma quaisquer alterações recentes no sistema ou em seu ambiente. Crie uma linha do tempo das mudanças recentes
	Histórico dos esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema por conta própria, certifique-se de registrar os passos que seguiu e o resultado obtido.

Solucionar problemas de objetos e storage

Confirme as localizações dos dados dos objetos no StorageGRID

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 conforme o esperado e se os dados do objeto estão sendo armazenados no local correto.

Antes de começar

- Você precisa ter um identificador de objeto, que pode ser um dos seguintes:
  - **UUID**: Identificador Único Universal do objeto. Insira o UUID em letras maiúsculas.
  - **CBID**: O identificador único do objeto no StorageGRID. Você pode obter o CBID de um objeto no log de auditoria. Insira o CBID em letras maiúsculas.
  - **Bucket S3 e chave do objeto**: Quando um objeto é ingerido através do "Interface S3", o aplicativo cliente usa uma combinação de bucket e chave do objeto para armazenar e identificar o objeto.

Passos

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

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

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

4. Selecione **Pesquisar**.

   O "resultados da pesquisa de metadados do objeto" aparece. Esta página lista os seguintes tipos de informação:

   - Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), o nome do objeto, o nome do contêiner, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e 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 chave-valor de metadados de usuário personalizados associados ao objeto.
   - Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
   - Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.

- Para cópias de objetos com código de apagamento, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, a localização do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, é exibida uma lista dos segmentos do objeto, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os 100 primeiros 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 têm garantia de persistência entre versões.

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

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```

Saiba mais sobre falhas de armazenamento de objetos para volumes de storage no StorageGRID

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

Você pode visualizar informações do armazenamento de objetos para cada Storage Node. Selecione **Nodes** > ***Storage Node*** > **Storage**.

Disk devices

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

Volumes

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

Object stores

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

Dependendo da natureza da falha, problemas com um volume de armazenamento podem ser refletidos em "alertas de volume de armazenamento". Se um volume de armazenamento falhar, você deve reparar o volume de armazenamento com falha para restaurar o Nó de Armazenamento à funcionalidade completa o mais rápido possível. Se necessário, você pode acessar a guia **Configuração** e "Coloque o nó de armazenamento em um estado somente leitura" para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto você se prepara para uma recuperação completa do servidor.

Verifique a integridade dos dados do objeto no StorageGRID

O sistema StorageGRID verifica a integridade dos dados dos objetos nos nós de armazenamento, verificando tanto objetos corrompidos quanto ausentes.

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

O que é verificação de antecedentes?

O processo de verificação em segundo plano verifica automática e continuamente os nós de armazenamento em busca de cópias corrompidas de dados de objetos e tenta reparar automaticamente quaisquer problemas que encontrar.

A verificação em segundo plano verifica a integridade de objetos replicados e objetos com código de apagamento, da seguinte forma:

- **Objetos replicados**: Se o processo de verificação em segundo plano encontrar um objeto replicado corrompido, a cópia corrompida é removida de sua localização e colocada em quarentena em outro local no Storage Node. Em seguida, uma nova cópia íntegra é gerada e alocada para atender às políticas ILM ativas. A nova cópia pode não ser alocada no Storage Node que foi usado para a cópia original.

  > ⓘ Os dados de objetos corrompidos são colocados em quarentena em vez de serem excluídos do sistema, permitindo que ainda sejam acessados. Para obter mais informações sobre como acessar dados de objetos em quarentena, entre em contato com o suporte técnico.

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

  O processo de verificação em segundo plano verifica apenas objetos em Storage Nodes. Ele não verifica objetos em um Cloud Storage Pool. Os objetos devem ter mais de quatro dias para serem elegíveis para verificação em segundo plano.

A verificação em segundo plano é executada continuamente, de forma a não interferir com as atividades normais do sistema. A verificação em segundo plano não pode ser interrompida. No entanto, você pode aumentar a frequência da verificação em segundo plano para verificar mais rapidamente o conteúdo de um Storage Node caso suspeite de algum problema.

Alertas relacionados à verificação em segundo plano

Se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente (porque a corrupção impede a identificação do objeto), o alerta **Unidentified corrupt object detected** será acionado.

Se a verificação em segundo plano não conseguir substituir um objeto corrompido porque não localizar outra cópia, o alerta **Objetos potencialmente perdidos** será acionado.

O que é verificação de existência de objeto?

A verificação de existência de objetos verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados para apagamento existem em um nó de armazenamento. A verificação de existência de objetos não verifica os dados do objeto em si (isso é feito pela verificação em segundo plano); em vez disso, ela fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware puder ter afetado a integridade de 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 objetos lê os metadados de cada objeto armazenado no StorageGRID e verifica a existência tanto de cópias replicadas do objeto quanto de fragmentos de objeto codificados para apagamento. Quaisquer dados ausentes são tratados da seguinte forma:

- **Cópias replicadas**: Se uma cópia dos dados de um objeto replicado estiver faltando, StorageGRID tenta automaticamente substituir a cópia por uma cópia armazenada em outro local do sistema. O Storage Node executa uma avaliação ILM em uma cópia existente, 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 atender às políticas ILM ativas do sistema. Essa nova cópia pode não ser colocada no mesmo local onde a cópia ausente estava armazenada.
- **Fragmentos codificados para apagamento**: Se um fragmento de um objeto codificado para apagamento estiver faltando, StorageGRID tenta automaticamente reconstruir o fragmento ausente no mesmo nó de armazenamento usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), ILM tenta encontrar outra cópia do objeto, que pode ser usada para gerar um novo fragmento codificado para apagamento.

Executar verificação de existência de objeto

Você cria e executa uma tarefa de verificação de existência de objeto por vez. Ao criar uma tarefa, você seleciona os Storage Nodes e os volumes que deseja verificar. Você também seleciona a consistência da tarefa.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso de manutenção ou root".
- Você verificou se os Storage Nodes que deseja verificar estão online. Selecione **Nodes** para visualizar a tabela de nós. Certifique-se de que nenhum ícone de alerta apareça ao lado do nome do nó para os nós que você deseja verificar.
- Você se certificou de que os seguintes procedimentos **não** estão sendo executados nos nós que você deseja verificar:
  - Expansão do grid para adicionar um nó de armazenamento
  - Desativação do nó de armazenamento
  - Recuperação de um volume de armazenamento com falha

- Recuperação de um nó de armazenamento com uma unidade de sistema com falha
- Reequilíbrio de EC
- Clone de nó de appliance

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

Sobre esta tarefa

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

Passos

1. Selecione **Manutenção** > **Tarefas** > **Verificação de existência do objeto**.
2. Selecione **Criar tarefa**. 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 online, marque a caixa de seleção **Nome do nó** no cabeçalho da coluna.

   Você pode pesquisar pelo nome do nó ou pelo site.

   Você não pode selecionar nós que não estão conectados à grid.

4. Selecione **Continue**.
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 de cada nó selecionado, marque a caixa de seleção **Storage volume** no cabeçalho da coluna.

6. Selecione **Continue**.
7. Selecione a consistência para a tarefa.

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

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

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

8. Selecione **Continue**.
9. Revise e verifique suas seleções. Você pode selecionar **Anterior** para retornar a uma etapa anterior do assistente e atualizar suas seleções.

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

   - O trabalho é concluído.

- Você pausa ou cancela a tarefa. Você pode retomar uma tarefa que pausou, mas não pode retomar uma tarefa que cancelou.
- A tarefa foi interrompida. O alerta **A verificação de existência do objeto foi interrompida** foi acionado. Siga as ações corretivas especificadas para o alerta.
- A tarefa falha. O alerta **A verificação de existência do objeto falhou** é acionado. Siga as ações corretivas especificadas para o alerta.
- Uma mensagem de "Serviço indisponível" ou "Erro interno do servidor" é exibida. Após um minuto, atualize a página para continuar monitorando o job.

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

10. Enquanto a tarefa estiver em execução, visualize a guia **Tarefa ativa** e observe o valor de Cópias de objetos ausentes detectado.

    Este 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 detectadas for maior que 100, pode haver um problema com o armazenamento do Storage Node.

11. Após a conclusão do trabalho, execute quaisquer ações adicionais necessárias:
    - Se o número de cópias de objetos ausentes detectadas for zero, nenhum problema foi encontrado. Nenhuma ação é necessária.
    - Se o número de cópias de objetos ausentes detectadas for maior que zero e o alerta **Objetos potencialmente perdidos** não tiver sido acionado, então todas as cópias ausentes foram reparadas pelo sistema. Verifique se quaisquer problemas de hardware foram corrigidos para evitar danos futuros às cópias de objetos.
    - Se o número de cópias de objetos ausentes detectadas for maior que zero e o alerta **Objetos potencialmente perdidos** tiver sido acionado, a integridade de dados pode ser afetada. Entre em contato com o suporte técnico.
    - Você pode investigar possíveis cópias de objetos perdidas usando o grep para extrair as mensagens de auditoria do LLST: `grep LLST audit_file_name`.

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

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

    Quando StorageGRID tiver tido tempo para alcançar a consistência de metadados para os nós e volumes incluídos na tarefa, executar a tarefa novamente poderá corrigir cópias de objetos ausentes relatadas erroneamente ou fazer com que cópias de objetos adicionais sejam verificadas caso tenham sido omitidas.

    a. Selecione **Manutenção** > **Verificação de existência do objeto** > **Histórico de tarefas**.
    b. Determine quais tarefas estão prontas para serem executadas novamente:
        i. Consulte a coluna **Hora de término** para determinar quais tarefas foram executadas há mais de três semanas.

ii. Para essas tarefas, verifique a coluna Consistency control em busca de strong-site ou strong-global.

c. Selecione a caixa de seleção para cada tarefa que você deseja executar novamente e, em seguida, selecione **Executar novamente**.

d. No assistente de Repetição de Tarefas, revise os nós e volumes selecionados e a consistência.

e. Quando estiver pronto para executar as tarefas novamente, selecione **Executar novamente**.

A aba "Tarefas Ativas" é exibida. Todas as tarefas que você selecionou são executadas novamente como uma única tarefa, com consistência de strong-site. Um campo **Tarefas Relacionadas** na seção Detalhes lista os IDs das tarefas originais.

Resolver o alerta de tamanho de objeto PUT do S3 muito grande no StorageGRID

O alerta "Tamanho do objeto S3 PUT muito grande" é acionado se um locatário tentar uma operação PutObject não multipart que exceda o limite de tamanho do S3 de 5 GiB.

Antes de começar

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

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

Passos

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

   a. Digite `ssh admin@primary_Admin_Node_IP`

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

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

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

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

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

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

Opção	Destino
Nós locais (padrão)	`/var/local/log/localaudit.log`
Nós administrativos/nós locais	• Nós de administração (primário e não primário): `/var/local/audit/export/audit.log` • Todos os nós: O arquivo `/var/local/log/localaudit.log` geralmente está vazio ou ausente nesse modo.

Opção	Destino
Servidor syslog externo	`/var/local/log/localaudit.log`

Dependendo das configurações de destino do seu log de auditoria, digite: `cd /var/local/log` ou `/var/local/audit/export/`

Para saber mais, consulte "Selecione o local do log".

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

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

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

Código	Descrição
SAIP	Endereço IP de origem
S3AI	ID do tenant
S3BK	Bucket
S3KY	Objeto
CSIZ	Tamanho (bytes)

Exemplo de resultados do log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

a. Acesse **Suporte** > **Ferramentas** > **Coleta de logs**. Colete os logs do aplicativo para o Storage Node no alerta. Especifique 15 minutos antes e depois do alerta. Consulte "Coletar arquivos de log e dados

do sistema".

b. Extraia o arquivo e acesse `bycast.log`:

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

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

Exemplo de 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 os inquilinos que o tamanho máximo de PutObject é de 5 GiB e que devem usar uploads multipartes para objetos maiores que 5 GiB.
5. Ignore o alerta por uma semana se o aplicativo tiver sido alterado.

Solucionar problemas de dados de objetos perdidos ou ausentes

Saiba mais sobre dados de objetos perdidos e extraviados no StorageGRID

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

O sistema StorageGRID utiliza informações de localização nos metadados de um objeto para determinar de qual local recuperar o objeto. Se uma cópia do objeto não for encontrada no local esperado, o sistema tenta recuperar outra cópia do objeto de outro local no sistema, desde que a política ILM contenha uma regra para criar duas ou mais cópias do objeto.

Se essa recuperação for bem-sucedida, o sistema StorageGRID substitui a cópia ausente do objeto. Caso contrário, o alerta **Objetos potencialmente perdidos** é acionado, da seguinte forma:

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

Você deve investigar imediatamente todos os alertas de **Objetos potencialmente perdidos** para determinar a causa raiz da perda e verificar se o objeto ainda pode existir em um Storage Node offline ou indisponível no momento. Consulte "Investigue objetos potencialmente perdidos". Alertas de objetos perdidos podem ser acionados falsamente por precaução.

No caso de perda de dados de objetos sem cópias, não há solução de recuperação. No entanto, você deve "Reinicie o contador de objetos potencialmente perdidos" evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos.

Quando o alerta **Objetos potencialmente perdidos** for acionado, você deve investigar imediatamente. Reúna informações sobre os objetos afetados e entre em contato com o suporte técnico.

Antes de começar

- Você precisa estar conectado ao Grid Manager usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você precisa ter o arquivo `Passwords.txt`.

Sobre esta tarefa

O alerta **Objetos potencialmente perdidos** indica que, de acordo com as informações disponíveis no StorageGRID, não existem cópias de um objeto na grid. Os dados podem ter sido perdidos permanentemente.

Investigue imediatamente os alertas de objetos perdidos. Pode ser necessário tomar medidas para evitar mais perda de dados. Em alguns casos, você poderá restaurar um objeto perdido se agir prontamente.

> Se forem reportados mais de 10 objetos como perdidos, entre em contato com o suporte técnico. Não siga este procedimento você mesmo.

Passos

1. Selecione **Nós**.
2. Selecione ***Nó de armazenamento*** > **Objetos**.
3. Confira o número de objetos perdidos mostrado na tabela de contagem de objetos.

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

4. A partir de um nó de administração, "Acesse o log de auditoria" para determinar o identificador único (UUID) do objeto que acionou o alerta **Objetos potencialmente perdidos**:
   a. Faça login no nó da grid:
      i. Digite o seguinte comando: `ssh admin@grid_node_IP`
      ii. Digite a senha listada no arquivo `Passwords.txt`.
      iii. Digite o seguinte comando para alternar para root: `su -`
      iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você estiver conectado como root, o prompt muda de `$` para `#`.
   b. Altere para o diretório onde os logs de auditoria estão localizados.

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

Opção	Destino
Nós locais (padrão)	`/var/local/log/localaudit.log`

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

Dependendo das configurações de destino do seu log de auditoria, digite: `cd /var/local/log` ou `/var/local/audit/export/`

Para saber mais, consulte "Selecione o local do log".

c. Use o comando grep para extrair as mensagens de log de auditoria de Object Lost (OLST). Digite: `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. Consulte os metadados do objeto perdido usando o UUID:

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

b. Insira o UUID e selecione **Pesquisar**.

c. Analise as localizações nos metadados e tome a ação apropriada:

Metadados	Conclusão
Objeto <object_identifier> não encontrado	Se o objeto não for encontrado, a mensagem "ERROR":"" será retornada. Se o objeto não for encontrado, Reinicie o contador de objetos potencialmente perdidos para limpar o alerta. A ausência do objeto indica que o objeto foi excluído intencionalmente.

Metadados	Conclusão
Locais > 0	Se houver locais listados na saída, o alerta **Objetos potencialmente perdidos** pode ser um falso positivo. Confirme se os objetos existem. Use o ID do nó e o caminho do arquivo listados na saída para confirmar que o arquivo de objeto está no local listado. Se os objetos existirem, Reinicie o contador de objetos potencialmente perdidos limpe o alerta.
Locais = 0	Se não houver locais listados na saída, o objeto pode estar faltando. Entre em contato com o suporte técnico. O suporte técnico pode pedir que você verifique se há um procedimento de recuperação de armazenamento em andamento. Veja as informações sobre "restaurando dados de objetos usando o Grid Manager" e "restaurando dados de objetos para um volume de armazenamento".

6. Após resolver os problemas com objetos perdidos, redefina o contador de objetos potencialmente perdidos para garantir que os alertas não sejam falsos positivos:
   a. Selecione **Nós**.
   b. Selecione ***Nó de armazenamento*** > **Tarefas**.
   c. Na seção Redefinir contador de objetos potencialmente perdidos, selecione **Redefinir**.

Resolver o alerta de storage de dados insuficiente no StorageGRID

O alerta **Armazenamento de dados de objetos insuficiente** monitora quanto espaço está disponível para armazenar dados de objetos em cada Storage Node.

Antes de começar

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

Sobre esta tarefa

O alerta **Baixo espaço de armazenamento de dados de objetos** é acionado quando a quantidade total de dados de objetos replicados e codificados por eliminação em um Storage Node atende a uma das condições configuradas na regra de alerta.

Por padrão, um alerta importante 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
```

Nessa condição:

- `storagegrid_storage_utilization_data_bytes` é uma estimativa do tamanho total dos dados de objetos replicados e codificados para apagamento em um Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes`é a quantidade total de espaço de storage de objetos restante para um Storage Node.

Se um alerta importante ou secundário de **Armazenamento de dados de objeto insuficiente** for acionado, você deve executar um procedimento de expansão o mais rápido possível.

Passos

1. Selecione **Alertas** > **Atual**.

   A página de Alertas aparece.

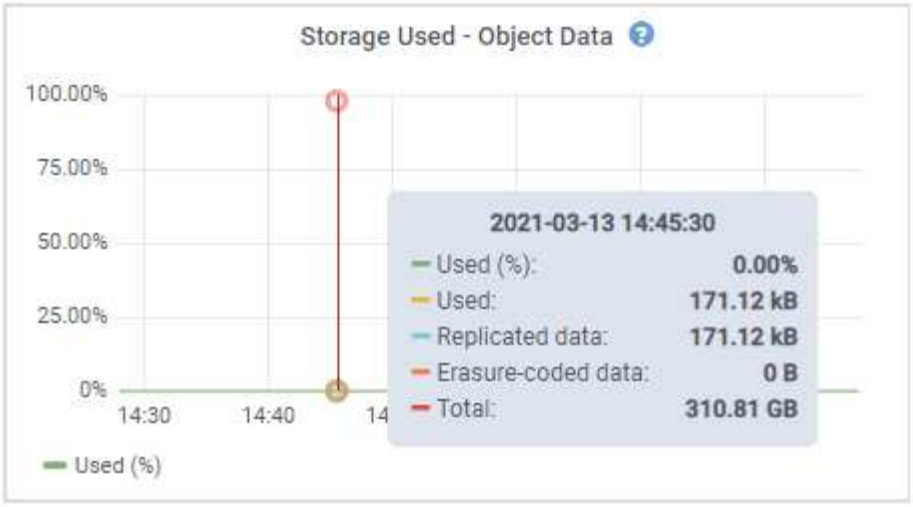
2. Na tabela de alertas, expanda o grupo de alertas **Low object data storage**, se necessário, e selecione o alerta que você deseja visualizar.

   Selecione o alerta, não o título de um grupo de alertas.

3. Analise os detalhes na caixa de diálogo e observe o seguinte:
   - Acionado por tempo
   - O nome do site e do nó
   - Os valores atuais das métricas para este alerta
4. Selecione **Nodes** > ***Storage Node or Site*** > **Storage**.
5. Posicione o cursor sobre o gráfico "Armazenamento Utilizado - Dados do Objeto".

   Os seguintes valores são exibidos:

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



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

   Analisar o uso do storage ao longo do tempo pode ajudar você a entender quanto storage foi utilizado antes e depois do alerta ser acionado e pode ajudar você a estimar quanto tempo pode levar para que o espaço restante do nó fique cheio.

7. Assim que possível, "adicionar capacidade de storage" para o seu grid.

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

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

Resolver o alerta de sobreposição de marca d'água no StorageGRID

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

Em versões anteriores, as três "marcas d'água de volume de armazenamento" eram configurações globais — os mesmos valores eram aplicados a todos os volumes de armazenamento em todos os Storage Nodes. A partir do StorageGRID 11.6, o software pode otimizar essas marcas d'água para cada volume de armazenamento, com base no tamanho do Storage Node e na capacidade relativa do volume.

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

- Seu sistema está próximo da capacidade máxima e não conseguiria aceitar novos dados se marcas d'água otimizadas fossem aplicadas. StorageGRID não alterará as configurações de marca d'água neste caso.
- Você definiu anteriormente alguma das marcas d'água do volume de armazenamento com um valor personalizado. StorageGRID não substituirá as configurações de marca d'água personalizadas por valores otimizados. No entanto, StorageGRID poderá acionar o alerta **Substituição de marca d'água somente leitura baixa** se o valor personalizado para a marca d'água somente leitura flexível do volume de armazenamento for muito pequeno.

Entenda o alerta

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

Cada ocorrência do alerta indica que o valor personalizado da marca d'água de leitura flexível do volume de armazenamento é menor que o valor mínimo otimizado para esse Storage Node. Se você continuar usando a configuração personalizada, o Storage Node pode ficar com pouco espaço disponível antes de conseguir fazer a transição segura para o estado somente leitura. Alguns volumes de armazenamento podem se tornar inacessíveis (desmontados automaticamente) quando o node atingir a capacidade.

Por exemplo, suponha que você tenha definido anteriormente o limite de tamanho somente leitura do volume de armazenamento para 5 GB. Agora, suponha que StorageGRID tenha calculado os seguintes valores otimizados para os quatro volumes de armazenamento no Storage Node A:

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

O alerta **Substituição de limite de leitura baixo** foi acionado para o Storage Node A porque seu limite personalizado (5 GB) é menor que o valor mínimo otimizado para todos os volumes nesse nó (11 GB). Se você continuar usando a configuração personalizada, o nó pode ficar criticamente com pouco espaço antes de conseguir fazer a transição para o estado somente leitura com segurança.

Resolver o alerta

Siga estas etapas se um ou mais alertas de **Substituição de watermark somente leitura de baixo nível** tiverem sido acionados. Você também pode usar estas instruções se estiver usando configurações de watermark personalizadas e quiser começar a usar configurações otimizadas, mesmo que nenhum alerta tenha sido acionado.

Antes de começar

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

Sobre esta tarefa

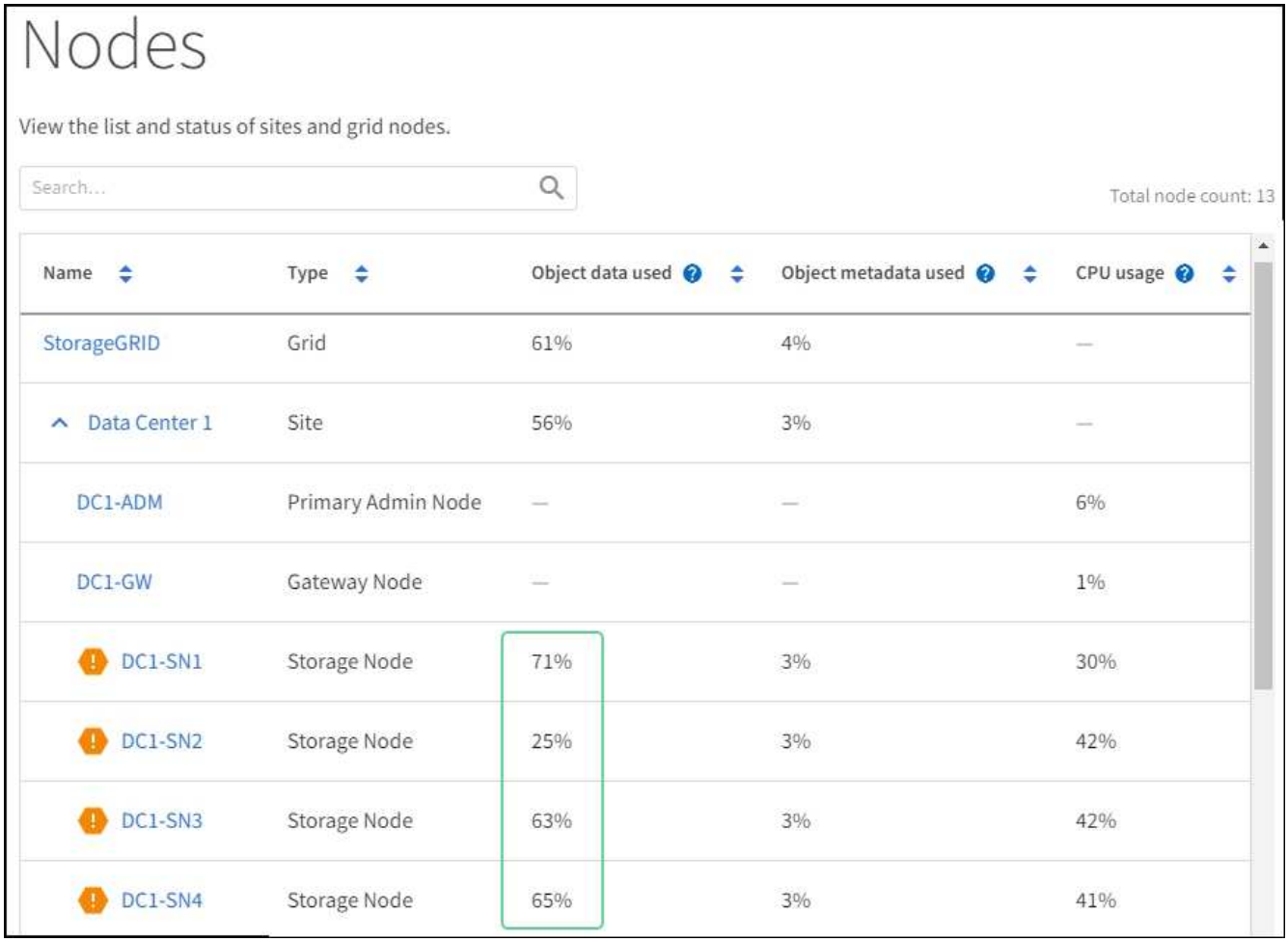
Você pode resolver o alerta **Substituição de marca d'água somente leitura baixa** atualizando as configurações de marca d'água personalizadas para as novas substituições de marca d'água. No entanto, se um ou mais Storage Nodes estiverem quase cheios ou se você tiver requisitos especiais de ILM, primeiro visualize as marcas d'água de armazenamento otimizadas e determine se é seguro usá-las.

Avalie o uso de dados de objetos para toda a grid

Passos

1. Selecione **Nós**.

2. Para cada site na grade, expanda a lista de nós.
3. Analise os valores percentuais apresentados na coluna **Dados do objeto utilizados** para cada Storage Node em cada site.



4. Siga a etapa apropriada:
   a. Se nenhum dos nós de armazenamento estiver próximo da capacidade máxima (por exemplo, todos os valores de **Dados de objeto usados** forem inferiores a 80%), você pode começar a usar as configurações de substituição. Acesse Use marcas d'água otimizadas.
   b. Se as regras do ILM usarem comportamento de ingestão estrito ou se determinados pools de armazenamento estiverem quase cheios, execute as etapas em Visualizar marcas d'água de storage otimizadas e Verifique se você pode usar marcas d'água otimizadas.

Visualizar marcas d'água de armazenamento otimizadas

StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que calculou para a marca d'água de leitura somente leitura suave do volume de storage. Você pode visualizar os valores otimizados mínimo e máximo para cada Storage Node em sua grid.

Passos

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

`storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark`

A última coluna mostra o valor mínimo otimizado da marca d'água de leitura somente leitura flexível para todos os volumes de armazenamento em cada Storage Node. Se esse valor for maior que a configuração personalizada para a marca d'água de leitura somente leitura flexível do volume de armazenamento, o alerta **Low read-only watermark override** será acionado para o Storage Node.

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

   `storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark`

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

5. Observe o valor máximo otimizado para cada Storage Node.

Determine se você pode usar marcas d'água otimizadas

Passos

1. Selecione **Nós**.
2. Repita estes passos para cada nó de armazenamento online:
   a. Selecione ***Nó de armazenamento*** > **Armazenamento**.
   b. Desça a página até a tabela de armazenamento de objetos.
   c. Compare o valor **Disponível** para cada armazenamento de objetos (volume) com a marca d'água otimizada máxima que você anotou para esse Storage Node.
3. Se pelo menos um volume em cada nó de armazenamento online tiver mais espaço disponível do que a marca d'água otimizada máxima para esse nó, acesse Use marcas d'água otimizadas para começar a usar as marcas d'água otimizadas.

   Caso contrário, expanda a grid o mais rápido possível. Ou "adicionar volumes de storage" para um nó existente ou "Adicionar novos Storage Nodes". Em seguida, vá para Use marcas d'água otimizadas para atualizar as configurações de watermark.

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

> Os mesmos valores de marca d'água personalizados são aplicados a todos os volumes de armazenamento em todos os Storage Nodes. O uso de valores menores do que os recomendados para as marcas d'água dos volumes de armazenamento pode fazer com que alguns volumes de armazenamento se tornem inacessíveis (desmontados automaticamente) quando o nó atingir a capacidade.

Usar marcas d'água otimizadas

Passos

1. Acesse **Suporte** > **Outros** > **Marcos de armazenamento**.
2. Selecione a caixa de seleção **Usar valores otimizados**.
3. Selecione **Salvar**.

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

Solucione problemas de metadados no StorageGRID

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

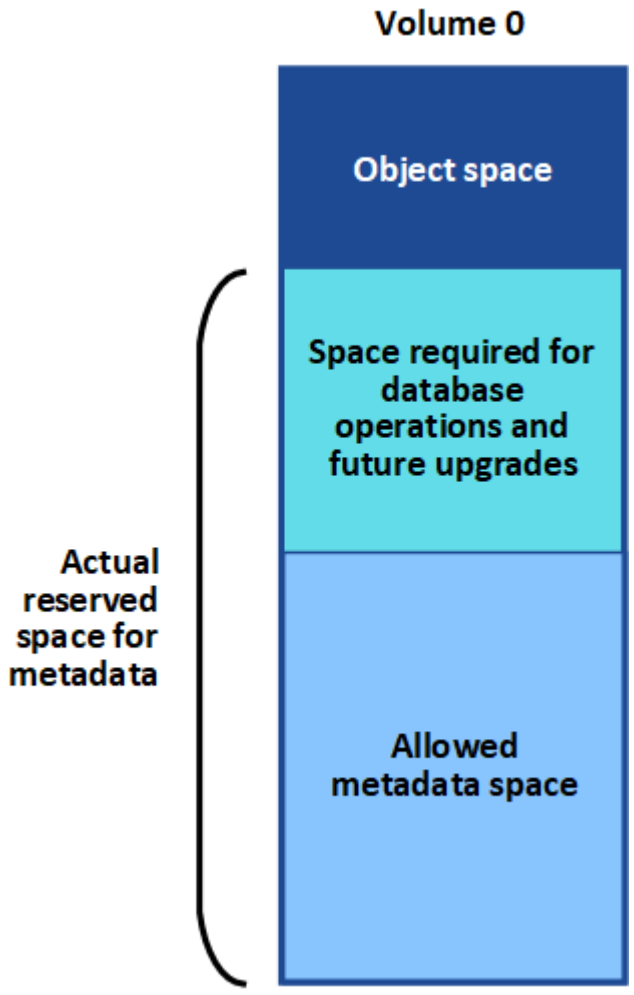
Antes de começar

Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

Sobre esta tarefa

Siga as ações recomendadas para cada alerta relacionado a metadados que for acionado. Se o alerta **Armazenamento de metadados insuficiente** for acionado, você deve adicionar novos Storage Nodes.

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



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 "monitorar a capacidade de metadados de objetos para cada Storage Node" para ajudar você a antecipar erros e corrigi-los antes que ocorram.

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

- **Menor**: os metadados do objeto estão utilizando 70% ou mais do espaço de metadados permitido. Você deve adicionar novos Storage Nodes o mais rápido possível.
- **Grave**: os metadados de objetos estão utilizando 90% ou mais do espaço de metadados permitido. Você deve adicionar novos Storage Nodes imediatamente.

> Quando os metadados de objetos estiverem utilizando 90% ou mais do espaço de metadados permitido, um aviso aparecerá no painel. Se esse aviso aparecer, você deve adicionar novos Storage Nodes imediatamente. Você nunca deve permitir que os metadados de objetos utilizem mais de 100% do espaço permitido.

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

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

Passos

1. Selecione **Alertas** > **Atual**.
2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de metadados insuficiente**, se necessário, e selecione o alerta específico que você deseja visualizar.
3. Analise os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **pouco armazenamento de metadados** for acionado, execute uma expansão para adicionar Storage Nodes imediatamente.

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

Após você realizar a expansão, o StorageGRID redistribui os metadados de objetos existentes para os novos nós, o que aumenta a capacidade geral de metadados do grid. Nenhuma ação do usuário é necessária. O alerta **Low metadata storage** é removido.

Solucionar problemas de erros de certificado no StorageGRID

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

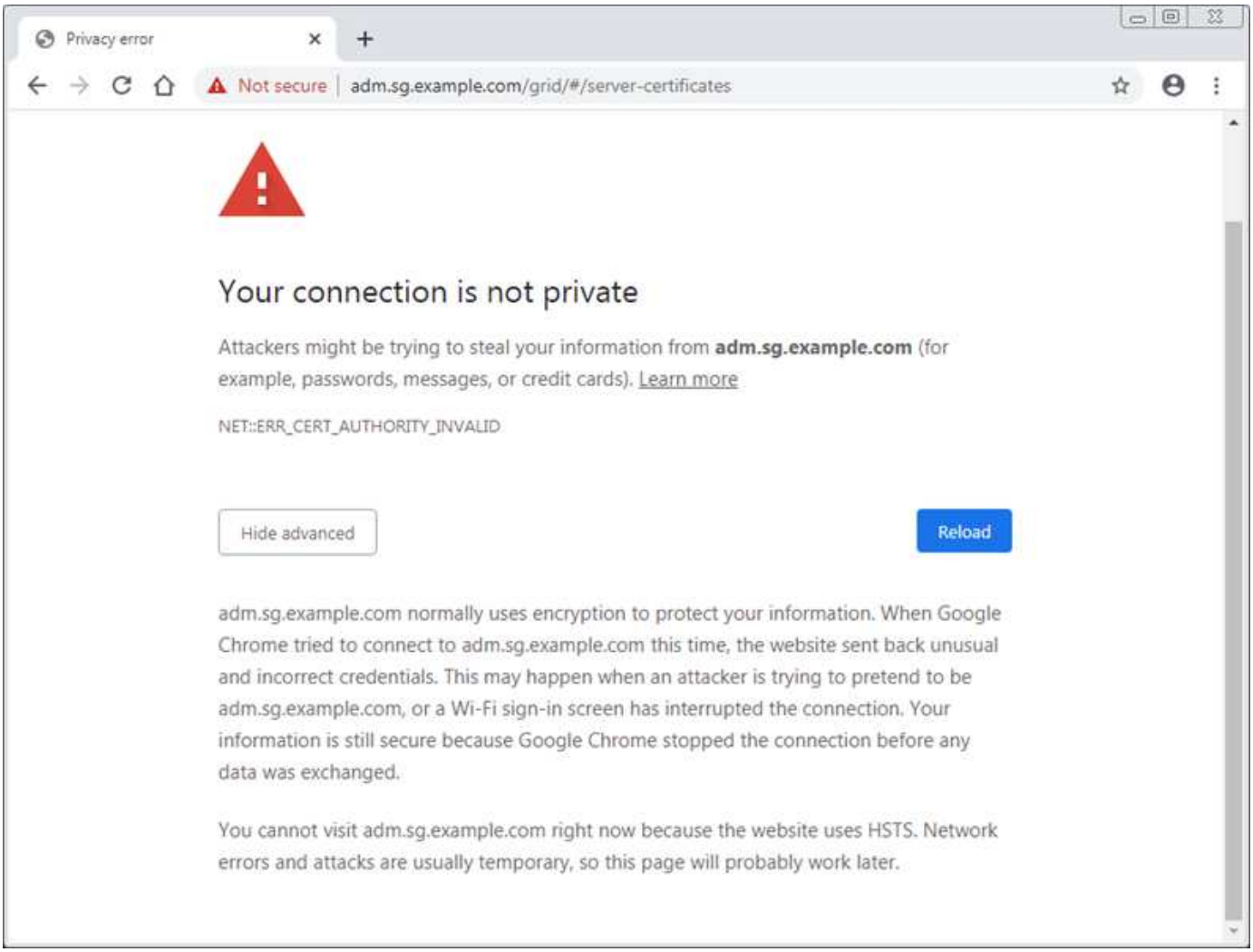
Sobre esta tarefa

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

Se você estiver acessando o Grid Manager ou o Tenant Manager usando um nome de domínio em vez de um endereço IP, o navegador exibirá um erro de certificado sem opção para ignorá-lo caso ocorra uma das seguintes situações:

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

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



Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração do certificado do servidor para a interface de gerenciamento** é acionado quando o certificado do servidor está prestes a expirar.

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

Passos

Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado: Selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, "Selecione a guia de certificado apropriada".

1. Verifique o período de validade do certificado. + Alguns navegadores da web e clientes S3 não aceitam certificados com um período de validade superior a 398 dias.
2. Se o certificado expirou ou expirará em breve, faça o upload ou gere um novo certificado.
   - Para obter um certificado de servidor, consulte as etapas para "Configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager".
   - Para um certificado de cliente, veja as etapas para "Configurando um certificado de cliente".
3. Para erros de certificado do servidor, tente uma ou ambas as opções a seguir:
   - Certifique-se de que o Nome Alternativo do Assunto (SAN) do certificado esteja preenchido e que o SAN corresponda ao endereço IP ou nome do host do nó ao qual você está se conectando.
   - Se você estiver tentando se conectar ao StorageGRID usando um nome de domínio:
     i. Insira o endereço IP do Nó de Administração em vez do nome de domínio para contornar o erro de conexão e acessar o Gerenciador de Grade.
     ii. No Gerenciador de Grade, selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, "Selecione a guia de certificado apropriada" para instalar um novo certificado personalizado ou continuar com o certificado padrão.
     iii. Nas instruções para administrar StorageGRID, consulte as etapas para "Configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager".

Solucionar problemas do nó de administração e da interface de usuário no StorageGRID

Você pode executar diversas tarefas para ajudar a determinar a origem de problemas relacionados aos Nós de Administração e à interface de usuário do StorageGRID.

Erros de login no Admin Node

Se você encontrar um erro ao fazer login em um StorageGRID Admin Node, seu sistema pode estar com um problema de "rede" ou "hardware" problema, um problema com "Serviços do nó de administração", ou um "problema com o banco de dados Cassandra" nos Storage Nodes conectados.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o arquivo `Passwords.txt`.
- Você tem "permissões de acesso específicas".

Sobre esta tarefa

Utilize estas diretrizes de resolução de problemas caso veja alguma das seguintes mensagens de erro ao tentar iniciar sessão em um Admin Node:

- `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 Administração, tente iniciar sessão no Gerenciador de Grade a partir de outro Nó de Administração para verificar o status de um Nó de Administração indisponível.
   - Se você conseguir fazer login, poderá usar as opções **Painel**, **Nós**, **Alertas** e **Suporte** para ajudar a determinar a causa do erro.
   - Se você tiver apenas um nó de administrador ou ainda não conseguir fazer login, vá para a próxima etapa.
3. Determine se o hardware do nó está offline.
4. Se o login único (SSO) estiver ativado para o seu sistema StorageGRID, consulte as etapas para "Configurando single sign-on".

   Pode ser necessário desativar e reativar temporariamente o SSO para um único Admin Node para resolver quaisquer problemas.

   > Se o SSO estiver ativado, você não pode fazer login usando uma porta restrita. Você deve usar a porta 443.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   A saída no terminal indica onde o arquivo de log foi copiado.

10. Revise os seguintes logs:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. Caso você não tenha identificado nenhum problema com o Nó de Administração, execute um dos seguintes comandos para determinar os endereços IP dos três Nós de Armazenamento que executam o serviço ADC em seu site. Normalmente, esses são os três primeiros Nós de Armazenamento instalados no site.

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

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

    Os nós administrativos utilizam o serviço ADC durante o processo de autenticação.

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

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

14. Repita os passos Use Lumberjack para coletar logs e Revisar logs para revisar os logs nos Storage Nodes.
15. Se não conseguir resolver o problema, entre em contato com o suporte técnico.

    Forneça os logs que você coletou ao suporte técnico. Veja também "Referência de arquivos de log".

Problemas de interface de usuário

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

Passos

1. Certifique-se de estar usando um "navegador web compatível".
2. Limpe o cache do seu navegador.

   Limpar o cache remove recursos desatualizados usados pela versão anterior do StorageGRID e permite

que a interface de usuário volte a funcionar corretamente. Para obter instruções, consulte a documentação do seu navegador.

Solucione problemas de rede, hardware e plataforma no StorageGRID

Existem diversas tarefas que você pode executar para ajudar a determinar a origem de problemas relacionados à rede StorageGRID, hardware e plataforma.

[[422-unprocessable-entity-errors]]
== Erros "422: Entidade não processável"

O erro 422: Entidade não processável pode ocorrer por diferentes motivos. Verifique a mensagem de erro para determinar o que causou seu 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 Transport Layer Security (TLS) ao configurar a federação de identidade usando Windows Active Directory (AD).
	
	A opção **Não usar TLS** não é compatível com servidores AD que exigem assinatura LDAP. Você deve selecionar a opção **Usar STARTTLS** ou **Usar LDAPS** para TLS.

Mensagem de erro	Causa raiz e ação corretiva

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

Alerta de incompatibilidade de MTU da Grid Network

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

Sobre esta tarefa

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

Passos

1. O acesso SSH externo está bloqueado por padrão. Se necessário, "permitir acesso temporariamente".
2. Liste as configurações de MTU para eth0 em todos os nós.
   - Utilize a consulta fornecida no Grid Manager.
   - Navegue até *primary Admin Node IP address*`/metrics/graph` e insira a seguinte consulta: `node_network_mtu_bytes{device="eth0"}`
3. "Modifique as configurações de MTU" conforme necessário para garantir que sejam iguais para a interface de rede Grid (eth0) em todos os nós.
   - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

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

Utilize os seguintes argumentos para modificar o MTU em nós baseados em Linux ou VMware.

Argumentos posicionais	Descrição
`mtu`	O MTU a ser configurado. Deve estar no intervalo de 1280 a 9216.
`network`	As redes às quais o MTU será aplicado. Inclua um ou mais dos seguintes tipos de rede: • grid • administrador • cliente

+

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

4. Se você permitiu o acesso SSH externo, "bloquear acesso"quando terminar a tarefa.

Alerta de erro de quadro de recepção de rede de nó

Os alertas de **erro de quadro de recepção de rede do nó** podem ser causados por problemas de conectividade entre StorageGRID e seu hardware de rede. Esse alerta desaparece automaticamente depois que o problema subjacente é resolvido.

Sobre esta tarefa

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

- A correção de erros de encaminhamento (FEC) é necessária e não está em uso
- Incompatibilidade de MTU entre a porta do switch e a NIC
- Altas taxas de erro de enlace
- Estouro do buffer circular da NIC

Passos

1. Siga os passos de resolução de problemas para todas as causas potenciais deste alerta, considerando sua configuração de rede.
2. Execute as seguintes etapas dependendo da causa do erro:

Incompatibilidade de FEC

Estas etapas são aplicáveis somente para alertas de **erro de quadro de recepção de rede do nó** causados por incompatibilidade de FEC em appliances StorageGRID.

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

   Você não pode configurar as configurações de FEC nos appliances StorageGRID. Em vez disso, os appliances tentam descobrir e espelhar as configurações de FEC nas portas do switch às quais estão conectados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC podem não conseguir negociar uma configuração de FEC comum. Sem uma configuração de FEC comum, a rede voltará ao modo "no-FEC". Quando o FEC não está ativado, as conexões ficam mais suscetíveis a erros causados por ruído elétrico.

   Os appliances StorageGRID suportam Firecode (FC) e Reed Solomon (RS) FEC, assim como sem FEC.

Incompatibilidade de MTU entre a porta do switch e a NIC

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

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

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

Veja também "Alterar a configuração de MTU".

Altas taxas de erro de enlace

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

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

Estouro do buffer circular da NIC

Se o erro for um estouro do buffer circular da placa de rede, entre em contato com o suporte técnico.

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

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

Erros de sincronização de tempo

Você poderá encontrar problemas com a sincronização de tempo em seu grid.

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

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

Linux: problemas de conectividade de rede

Você poderá encontrar problemas de conectividade de rede para nós do StorageGRID hospedados em hosts Linux.

Clonagem de endereço MAC

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

redes como "true" no seu arquivo de configuração do nó. Essa configuração faz com que o endereço MAC do contêiner StorageGRID use o endereço MAC do host. Consulte as instruções para "criar arquivos de configuração de nó".

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

Para obter mais informações, consulte as instruções para "habilitando clonagem de MAC".

Modo promíscuo

Se você não deseja usar clonagem de endereço MAC e prefere permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes daqueles atribuídos pelo hipervisor, certifique-se de que as propriedades de segurança nos níveis do switch virtual e do grupo de portas estejam definidas como **Aceitar** para Modo Promíscuo, Alterações de Endereço MAC e Transmissões Falsificadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, então 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 "como configurar a rede do host".

Linux: o status do nó é "órfão"

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

Sobre esta tarefa

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

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

Passos

1. Verifique os registros do daemon de serviço e do nó órfão em busca de erros óbvios ou mensagens sobre encerramento inesperado.
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 é

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

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

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

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

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

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

Linux: solucionar problemas de suporte a IPv6

Pode ser necessário habilitar o suporte a IPv6 no kernel se você instalou nós do StorageGRID em hosts Linux e percebeu que os endereços IPv6 não foram atribuídos aos contêineres dos nós conforme o esperado.

Sobre esta tarefa

Para visualizar o endereço IPv6 atribuído a um nó da grid:

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

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

Passos

1. 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 seu sistema operacional para alterar as configurações de `sysctl`. Em seguida, altere o valor para 0 antes de continuar.

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

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

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

O resultado deve ser 1.

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

> Se o resultado for diferente de 1, este procedimento não se aplica. Contate o suporte técnico.

5. Saia do contêiner: `exit`

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

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

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

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

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

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

8. Execute estes comandos para reiniciar o contêiner StorageGRID:

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

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

Solucionar problemas de mensagens de erro do servidor syslog externo para StorageGRID

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 caso você tenha 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 e 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 o gerenciamento de logs e o servidor syslog externo"

Mensagem de erro	Descrição e ações recomendadas
Não foi 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 seja 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 consegue acessar os endereços IP do servidor DNS.
Conexão recusada	A conexão TCP ou TLS com o servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS do host, ou um firewall pode estar bloqueando o acesso. 1. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 2. Confirme que o host para o serviço syslog está executando um daemon syslog que está escutando na porta especificada. 3. Confirme se nenhum firewall está bloqueando o acesso às conexões TCP/TLS dos nós para o endereço IP e a porta do servidor syslog.
Rede inacessível	O servidor syslog não está em uma sub-rede diretamente conectada. Um roteador retornou uma mensagem de falha ICMP indicando que não conseguiu encaminhar as mensagens de teste dos nós listados para o servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de Sub-redes da Grid Network, as Listas de Sub-redes das Admin Networks e os gateways da Client Network. Confirme se eles estão configurados para rotear o tráfego para o servidor syslog pela interface de rede e gateway esperados (Grid, Admin ou Client).

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

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

Saiba mais sobre problemas de armazenamento em cache do balanceador de carga no StorageGRID

Saiba mais sobre possíveis problemas com armazenamento em cache do balanceador de carga e como solucioná-los.

Determine se uma solicitação foi um acerto do cache

- O cabeçalho X-Cache é definido na resposta às solicitações processadas pelo serviço de cache. Códigos possíveis:

- `HIT`: O objeto foi servido do cache
- `PARTIAL-HIT`: O bucket/chave tinha um registro no cache, mas nem todo o intervalo solicitado pôde ser fornecido a partir do cache
- `STALE`: O bucket/chave tinha um registro em cache, mas o objeto foi atualizado desde a última vez que foi servido a partir do cache.
- `MISS`: O objeto não estava no cache

- O `nginx-gw/endpoint-access.log.gz`registro da solicitação inclui "unix:/run/cache-svc/cache-svc.sock" para solicitações processadas pelo cache.
- O `cache-svc/cache-svc.log`relatório exibe uma mensagem como "Request 320390: completed successfully (acerto do cache)" ou "Request 320375: completed successfully (cache miss)." Encontre o caminho solicitado procurando outros registros com a mesma string "Request *<number>*".

Baixa taxa de acertos do cache

- Taxas baixas de acerto do cache podem ser esperadas quando uma nova carga de trabalho é adicionada ou quando o conjunto de trabalho acessado por uma carga de trabalho é alterado. Nessas situações, espera-se que a taxa de acertos aumente com o tempo.
- Se várias cargas de trabalho estiverem usando armazenamento em cache, considere adicionar políticas de classificação de tráfego para isolar partes das cargas de trabalho que estão sendo atendidas pelo cache. As métricas de taxa de acertos do cache estão disponíveis por política de classificação de tráfego. Se algumas cargas de trabalho não estiverem apresentando boas taxas de acertos do cache, considere movê-las para outros endpoints que não tenham armazenamento em cache habilitado.
- Avalie a taxa de remoção de itens do cache. Se o cache for muito pequeno para acomodar o conjunto de trabalho, ele apresentará altas taxas de remoção e poderá contribuir para taxas de acertos mais baixas.
- Opções para melhorar as taxas de acertos de determinadas cargas de trabalho podem estar disponíveis no âmbito do FPVR.

Baixo desempenho

- Avalie a taxa de acertos do cache. Taxas baixas de acertos do cache podem levar a um desempenho geral baixo.
- Avalie a taxa de remoção do cache. Durante a remoção, alguns recursos de storage são usados para remover objetos existentes do disco. Se o processo de remoção não acompanhar o acesso de novos objetos, o sistema pode atingir os limites máximos e começar a ignorar o cache.
- Verifique os limites da rede usando os diagnósticos "Uso de recebimento das interfaces de rede" e "Uso de transmissão das interfaces de rede".

Analisar registros de auditoria

Mensagens e logs de auditoria

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e dos arquivos de log do StorageGRID. Você pode usar essas informações para ler e analisar o histórico de auditoria da atividade do sistema.

Estas instruções são para administradores responsáveis por gerar relatórios de atividade e uso do sistema que exigem análise das mensagens de auditoria do sistema StorageGRID.

Para usar o arquivo de log de texto, você precisa ter acesso ao compartilhamento de auditoria configurado no nó de administração.

Para obter informações sobre como configurar os níveis de mensagens de auditoria e usar um servidor syslog externo, consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

Como as mensagens de auditoria se movem pelo sistema StorageGRID até o arquivo de log de auditoria para retenção

Todos os serviços do StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID até o arquivo `audit.log`.

Os fluxos de trabalho a seguir para mensagens de auditoria e retenção de mensagens de auditoria são aplicáveis somente se StorageGRID estiver configurado para **Admin Nodes/nós locais** ou **Admin Node e external syslog server**. Se StorageGRID estiver configurado para "Local nodes only" (padrão) ou "External syslog server", as mensagens de auditoria são salvas localmente em cada nó no `/var/local/log/localaudit.log` arquivo e não podem ser processadas pelos Admin Nodes ou Storage Nodes.

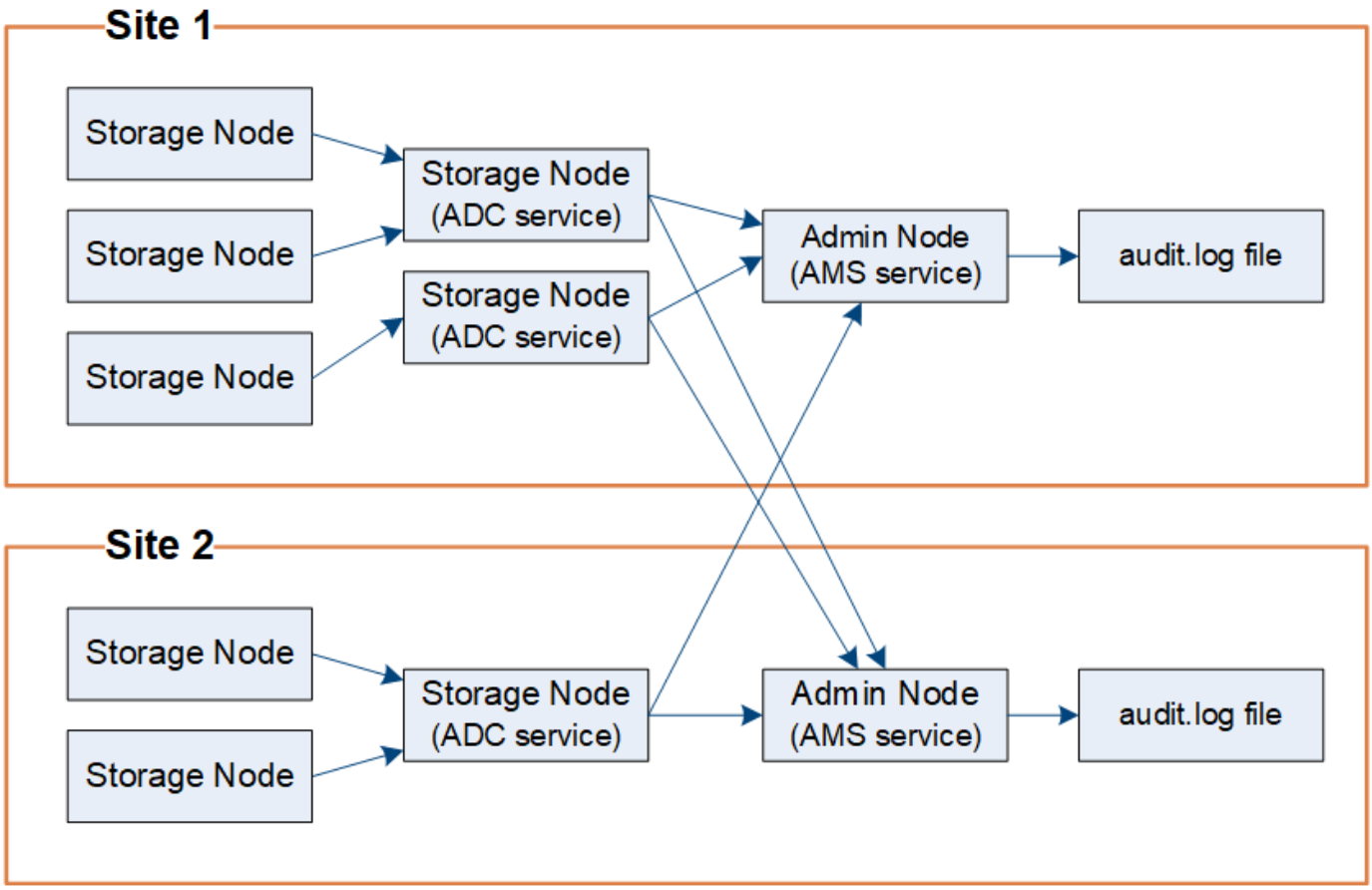
Fluxo de mensagens de auditoria

As mensagens de auditoria são processadas pelos Nós de Administração quando StorageGRID está configurado para **Nós de Administração/nós locais** ou **Nó de Administração e servidor syslog externo** e pelos Nós de Armazenamento que possuem um serviço de Controlador de Domínio Administrativo (ADC).

Conforme ilustrado no diagrama de fluxo de mensagens de auditoria, cada nó do StorageGRID envia suas mensagens de auditoria para um dos serviços ADC no data center. O serviço ADC é ativado automaticamente para os três primeiros nós de armazenamento instalados em cada site.

Por sua vez, cada serviço ADC atua como um repetidor e envia seu conjunto de mensagens de auditoria para cada Nó de Administração no StorageGRID, o que fornece a cada Nó de Administração um registro completo da atividade do sistema.

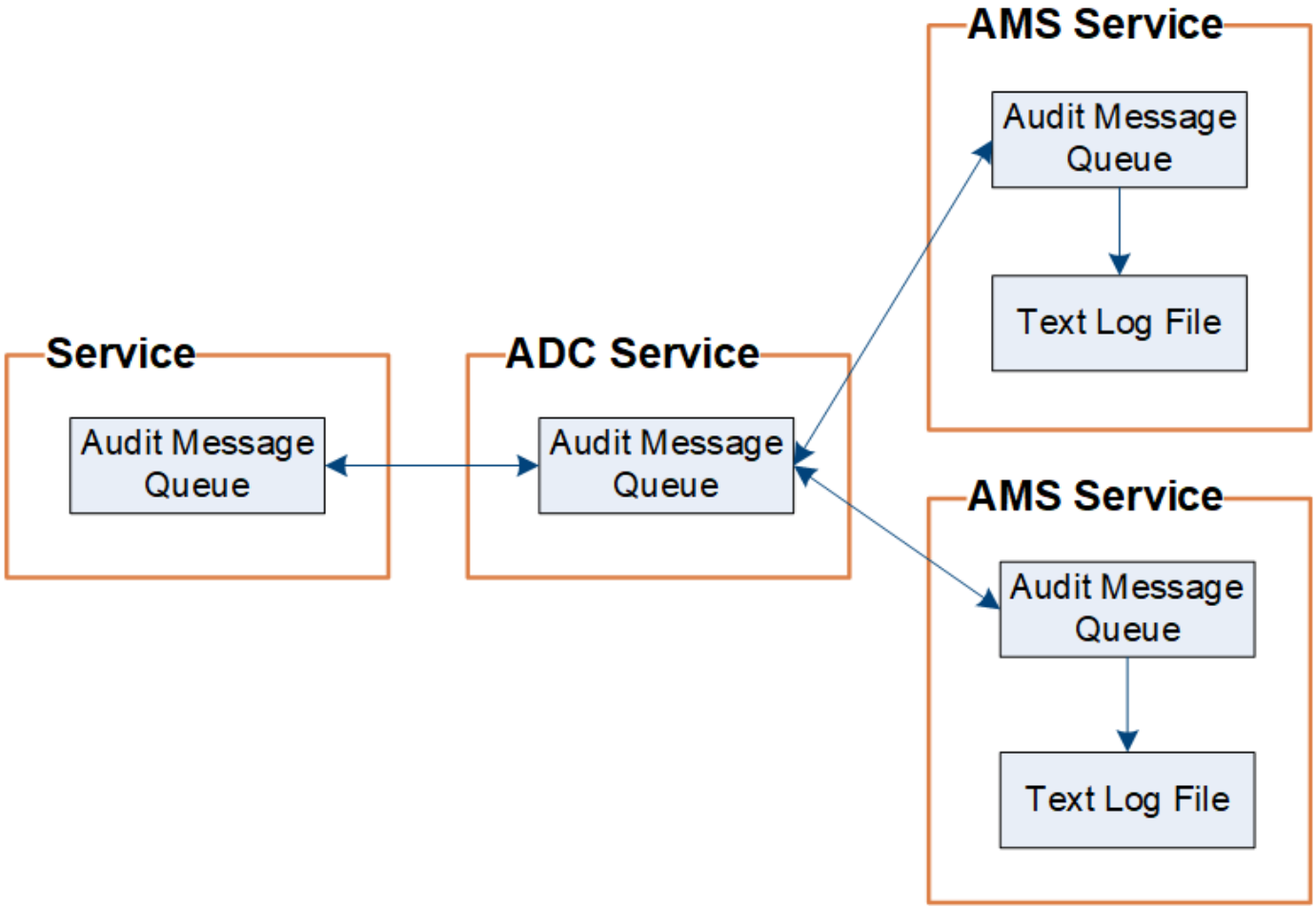
Cada nó de administração armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é nomeado `audit.log`.



Retenção de mensagens de auditoria

StorageGRID utiliza um processo de copiar e excluir para garantir que nenhuma mensagem de auditoria seja perdida antes de ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no diretório do Nó de Administração `/var/local/audit/export`. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conectividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, consomem mais do espaço disponível no diretório `/var/local/` de cada nó. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizam o processamento do seu backlog e ficam temporariamente indisponíveis para novas mensagens.

Especificamente, você poderá observar os seguintes comportamentos:

- Se o `/var/local/audit/export`diretório usado por um Nó de Administração ficar cheio, o Nó de Administração será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações do cliente S3 não são afetadas. O alarme XAMS (Unreachable Audit Repositories) é acionado quando um repositório de auditoria está inacessível.
- Se o `/var/local/` diretório usado por um Storage Node com o serviço ADC atingir 92% de sua capacidade, o nó será sinalizado como indisponível para mensagens de auditoria até que o diretório esteja com apenas 87% de sua capacidade ocupada. As solicitações de cliente S3 para outros nós não são afetadas. O alarme NRLY (Available Audit Relays) é acionado quando os relés de auditoria estão inacessíveis.

> Caso não haja nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente no arquivo `/var/local/log/localaudit.log`.

- Se o `/var/local/`diretório usado por um nó de armazenamento ficar 85% cheio, o nó começa a recusar solicitações de clientes S3 com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito:

- A interrupção de um Nó Administrativo ou de um Nó de Armazenamento com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar sobrecarregados.
- Uma taxa de atividade sustentada que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC fica cheio por motivos não relacionados a mensagens de auditoria. Quando isso acontece, o nó para de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme Audit Messages Queued (AMQS)

Para ajudar você a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **Fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de Storage Node ou Admin Node atinge determinados limites.

Se o alerta **Fila de auditoria grande** ou o alarme AMQS legado for acionado, comece verificando a carga do sistema—se houver um número significativo de transações recentes, o alerta e o alarme devem se resolver com o tempo e podem ser ignorados.

Se o alerta ou alarme persistir e aumentar em gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para Client Writes e Client Reads para Error ou Off. Veja "Configurar o gerenciamento de logs e o servidor syslog externo".

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora em caso de falha de rede ou de nó. Por esse motivo, mensagens duplicadas podem existir no log de auditoria.

Acesse os arquivos de log de auditoria a partir da linha de comando do nó Admin do StorageGRID

A pasta de auditoria contém o arquivo ativo `audit.log` e quaisquer arquivos de log de auditoria compactados. Você pode acessar os arquivos de log de auditoria diretamente da linha de comando do Admin Node.

O `audit.log`arquivo permanece vazio a menos que você configure StorageGRID para **Admin Nodes/nós locais** ou **Admin Node e servidor syslog externo**. Para mais informações, consulte "Selecione o local do log".

Antes de começar

- Você tem "permissões de acesso específicas".
- Você precisa ter o arquivo `Passwords.txt`.
- Você precisa saber o endereço IP de um Admin Node.

Passos

1. Faça login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no arquivo `Passwords.txt`.

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

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

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

2. Acesse o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/audit/export/
```

3. Visualize o arquivo de log de auditoria atual ou um arquivo salvo, conforme necessário.

Saiba mais sobre a rotação de arquivos de log de auditoria no StorageGRID

Se StorageGRID estiver configurado para **Nós de administração/nós locais** ou **Nó de administração e servidor syslog externo**, os arquivos de log de auditoria são salvos no diretório `/var/local/audit/export/` do Nó de administração. Os arquivos de log de auditoria ativos são nomeados `audit.log`.

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

Uma vez por dia, o arquivo `audit.log` ativo é salvo e um novo arquivo `audit.log` é iniciado. O nome do arquivo salvo indica quando ele foi salvo, no formato *`yyyy-mm-dd.txt`*. Se mais de um log de auditoria for criado em um único dia, os nomes dos arquivos usam a data em que o arquivo foi salvo, seguida por um número, no formato *`yyyy-mm-dd.txt.n`*. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são o primeiro e o segundo arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original. Com o tempo, o armazenamento do Admin Node alocado para os logs de auditoria é consumido. Um script monitora o consumo de espaço do log de auditoria e exclui arquivos de log conforme necessário para liberar espaço no diretório `/var/local/audit/export/`. Os logs de auditoria são excluídos com base na data em que foram criados. Os logs mais antigos são excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log`.

Este exemplo mostra o arquivo ativo `audit.log`, o arquivo do dia anterior (`2018-04-15.txt` e o arquivo compactado do dia anterior (`2018-04-14.txt.gz`.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato do arquivo de log de auditoria

Saiba mais sobre o formato dos arquivos de log de auditoria no StorageGRID

Os arquivos de log de auditoria são encontrados em cada nó administrativo e contêm

uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O Tempo Universal Coordenado (UTC) do evento que desencadeou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* são microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT`.

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha foram adicionadas para facilitar a leitura). Essas mensagens foram geradas quando um locatário criou um bucket S3 e adicionou dois objetos a esse bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
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::175300642415970547
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::175300642415970547
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 audit-explain" para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar o "ferramenta audit-sum" para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

Use a ferramenta audit-explain para traduzir as mensagens de auditoria do StorageGRID

Você pode usar a ferramenta `audit-explain` para traduzir as mensagens de auditoria no log de auditoria para um formato fácil de ler.

Antes de começar

- Você tem "permissões de acesso específicas".
- Você precisa ter o arquivo `Passwords.txt`.
- Você precisa 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 pelo suporte técnico durante operações de resolução de problemas. O processamento de `audit-explain`consultas pode consumir uma grande quantidade de poder de processamento 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 do S3 com ID de conta 92484777680322627870 usou solicitações PUT do S3 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 ferramenta `audit-explain`pode fazer o seguinte:

- Processar logs de auditoria simples ou compactados. Por exemplo:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Processar vários arquivos simultaneamente. Por exemplo:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o comando `grep` ou outros meios. Por exemplo:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando as partes que deseja examinar e executando `audit-explain` nessas partes, em vez de processar o

arquivo inteiro.

> A `audit-explain`ferramenta não aceita arquivos compactados como entrada via pipe. Para processar arquivos compactados, forneça os nomes dos arquivos como argumentos de linha de comando ou use a `zcat`ferramenta para descompactar os arquivos primeiro. Por exemplo:
>
> `zcat audit.log.gz | audit-explain`

Use a opção `help (-h)` para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Faça login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no arquivo `Passwords.txt`.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no arquivo `Passwords.txt`.

   Quando você está logado como root, o prompt muda de `$` para `#`.
2. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e o local do(s) arquivo(s) que você deseja analisar:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   A `audit-explain` ferramenta imprime interpretações legíveis por humanos de todas as mensagens no(s) arquivo(s) especificado(s).

   > Para reduzir o comprimento das linhas e facilitar a leitura, os carimbos de data/hora não são exibidos por padrão. Se você quiser ver os carimbos de data/hora, use a opção (`-t`timestamp.

Use a ferramenta audit-sum para resumir as mensagens de auditoria do StorageGRID

Você pode usar a `audit-sum` ferramenta para contar as mensagens de log de auditoria de gravação, leitura, head e exclusão e para ver o tempo (ou tamanho) mínimo, máximo e médio para cada tipo de operação.

Antes de começar

- Você tem "permissões de acesso específicas".
- Você tem o arquivo `Passwords.txt`.
- Você sabe 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 levaram.

A `audit-sum`ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de resolução de problemas. O processamento de `audit-sum`consultas pode consumir uma grande quantidade de poder de processamento 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 do protocolo levaram.

```
  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 horários para as seguintes mensagens de auditoria S3 e ILM em um log de auditoria.

Os códigos de auditoria são removidos do produto e da documentação à medida que os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do StorageGRID. Por exemplo, "StorageGRID 11.8 Usando a ferramenta audit sum".

Código	Descrição	Consulte
IDEL	Exclusão iniciada pelo ILM: registra quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket.	"SDEL: S3 DELETE"
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 HEAD"
SPUT	S3 PUT: registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"

A ferramenta `audit-sum` pode fazer o seguinte:

- Processar logs de auditoria simples ou compactados. Por exemplo:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Processar vários arquivos simultaneamente. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o comando `grep` ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Esta ferramenta não aceita arquivos compactados como entrada via pipe. Para processar arquivos compactados, forneça os nomes dos arquivos como argumentos de linha de comando ou use a ferramenta `zcat` para descompactar os arquivos primeiro. Por exemplo:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Você pode usar opções de linha de comando para resumir as operações em buckets separadamente das operações em objetos ou para agrupar resumos de mensagens por nome do bucket, por período ou por tipo de destino. Por padrão, os resumos mostram o tempo mínimo, máximo e médio de operação, mas você pode usar a opção `size (-s)` para visualizar o tamanho do objeto.

Use a opção `help (-h)` para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Faça login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Digite a senha listada no arquivo `Passwords.txt`.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no arquivo `Passwords.txt`.

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

2. Se você deseja analisar todas as mensagens relacionadas às operações de escrita, leitura, head e exclusão, siga estas etapas:

a. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e o local do(s) arquivo(s) que você deseja analisar:

```
$ audit-sum /var/local/audit/export/audit.log
```

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações do protocolo levaram.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Neste exemplo, as operações SGET (S3 GET) são as mais lentas em média, com 1,13 segundos, mas as operações SGET e SPUT (S3 PUT) apresentam tempos máximos longos, de cerca de 1.770 segundos.

b. Para exibir as 10 operações de recuperação mais lentas, use o comando grep para selecionar apenas as mensagens SGET e adicione a opção de saída longa (`-l` para incluir os caminhos dos objetos:

```
grep SGET audit.log | audit-sum -l
```

Os resultados incluem o tipo (objeto ou bucket) e o caminho, o que permite usar o grep para pesquisar no log de auditoria outras mensagens relacionadas a esses objetos específicos.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
A partir deste exemplo de saída, você pode ver que as três solicitações GET mais lentas do S3 foram para objetos com cerca de 5 GB, que são muito maiores do que os outros objetos. O tamanho grande explica os tempos de recuperação mais lentos no pior caso.

3. Se você deseja determinar os tamanhos dos objetos que estão sendo inseridos e recuperados da sua grade, use a opção size (`-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 dos objetos 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 é recuperada.

4. Se você quiser determinar se as recuperações foram lentas ontem:

   a. Execute 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 o tráfego GET no S3 apresentou um pico entre 06:00 e 07:00. Os tempos máximo e médio foram consideravelmente maiores durante esse período e não aumentaram gradualmente conforme a contagem aumentava. Essas métricas sugerem que a capacidade foi excedida, possivelmente na rede ou na capacidade do grid de processar as solicitações.

b. Para determinar o tamanho dos objetos recuperados a cada hora ontem, adicione a opção (`-s`size ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no máximo.

c. Para ver mais detalhes, use a "ferramenta audit-explain" para revisar 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 em várias linhas, adicione o comando `less` para exibir o conteúdo do arquivo de log de auditoria uma página (uma tela) por vez.

5. Se você deseja determinar se as operações SPUT em buckets são mais lentas do que as operações SPUT em objetos:

a. Comece usando a opção `-go` que agrupa as mensagens para operações de objeto e de bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Os resultados mostram que as operações SPUT para buckets têm características de desempenho diferentes das operações SPUT para objetos.

b. Para determinar quais buckets têm as operações SPUT mais lentas, use a opção `-gb` 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 opções `-gb` 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

Saiba mais sobre a estrutura das mensagens de auditoria do StorageGRID

As mensagens de auditoria trocadas dentro do sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou atividade relatada.

Caso as informações resumidas fornecidas pelas "audit-explain" e "soma de auditoria" ferramentas sejam insuficientes, consulte esta seção para entender o formato geral de todas as mensagens de auditoria.

O seguinte é um exemplo de mensagem de auditoria, como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Cada mensagem de auditoria contém uma sequência de elementos de atributo. Toda a sequência está entre colchetes (`[ ]`), e cada elemento de atributo na sequência possui as seguintes características:

- Entre colchetes `[ ]`
- Introduzido pela string `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 caracteres para o atributo que está sendo relatado. Existem alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos do evento.
- `type`é um identificador de quatro caracteres do tipo de dados de programação do valor, como UI64, FC32 e assim por diante. O tipo é delimitado por parênteses `( ).
- `value` é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores sempre seguem dois pontos (`:`). Os valores do tipo de dados CSTR são delimitados por aspas duplas " ".

Tipos de dados em mensagens de auditoria do StorageGRID

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Número inteiro longo sem sinal (32 bits); pode armazenar os números de 0 a 4.294.967.295.
UI64	Número inteiro longo duplo sem sinal (64 bits); pode armazenar os números de 0 a 18,446,744,073,709,551,615.
FC32	Constante de quatro caracteres; um valor inteiro sem sinal de 32 bits representado como quatro caracteres ASCII, como "ABCD".
IPAD	Utilizado para endereços IP.
CSTR	Uma matriz de caracteres UTF-8 de comprimento variável. Os caracteres podem ser escapados com as seguintes convenções: • A barra invertida é \\. • A quebra de linha é \r. • Aspas duplas são \". • A quebra de linha (nova linha) é \n. • Os caracteres podem ser substituídos por seus equivalentes hexadecimais (no formato \xHH, onde HH é o valor hexadecimal que representa o caractere).

Dados específicos do evento em mensagens de auditoria do StorageGRID

Cada mensagem de auditoria no log de auditoria registra dados específicos de um evento do sistema.

Após o `[AUDT:`contêiner inicial que identifica a própria mensagem, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrita pela mensagem de auditoria. Esses atributos estão destacados

no exemplo a seguir:

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

O `ATYP`elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o "SHEA"código da mensagem ([ATYP(FC32):SHEA]), indicando que foi gerada por uma solicitação S3 HEAD bem-sucedida.

Elementos comuns em mensagens de auditoria do StorageGRID

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
AMID	FC32	ID do módulo: um identificador de quatro caracteres 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. Esse ID não pode ser alterado.
ASES	UI64	Identificador da Sessão de Auditoria: em versões anteriores, este elemento indicava o momento em que o sistema de auditoria era inicializado após o serviço ser iniciado. Esse valor de tempo era 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.

Código	Tipo	Descrição
ASQN	UI64	Contador de Sequências: em versões anteriores, esse contador era incrementado para cada mensagem de auditoria gerada no nó da grade (ANID) e zerado ao reiniciar o serviço. **Nota:** Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: um identificador compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.
ATIM	UI64	Carimbo de data/hora: o momento em que o evento que disparou a mensagem de auditoria foi gerado, medido em microssegundos desde a época do sistema operacional (00:00:00 UTC de 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora em data e hora locais utiliza milissegundos. Pode ser necessário arredondar ou truncar o registro de data e hora. O horário legível 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 `T` é um caractere literal que indica o início do segmento de tempo da data. *`UUUUUU`* são microssegundos.
ATYP	FC32	Tipo de evento: um identificador de quatro caracteres do evento que está sendo registrado. Isso determina o conteúdo da "carga" da mensagem: os atributos que estão incluídos.
MÉDIA	UI32	Versão: a versão da mensagem de auditoria. À medida que o StorageGRID evolui, novas versões dos serviços podem incorporar novos recursos nos relatórios de auditoria. Este campo permite a compatibilidade com versões anteriores no serviço AMS para processar mensagens de versões mais antigas dos serviços.
RSLT	FC32	Resultado: o resultado do evento, processo ou transação. Se não for relevante para uma mensagem, usa-se NONE em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

Formato e exemplos de mensagens de auditoria do StorageGRID

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

Segue abaixo um exemplo de mensagem de auditoria que pode aparecer no arquivo `audit.log`:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo registrado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento foi registrado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

O valor do atributo ATYP é SPUT. "SPUT" representa uma transação PUT do S3, que registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o bucket ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Para descobrir quando o evento PUT ocorreu, observe o carimbo de data/hora UTC (Tempo Universal Coordenado) no início da mensagem de auditoria. Esse 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]]
```

O ATIM registra o tempo, em microssegundos, desde o início da época UNIX. No exemplo, o valor `1405631878959669` corresponde a quinta-feira, 17 de julho de 2014 21:17:59 UTC.

Mensagens de auditoria e o ciclo de vida do objeto

Quando as mensagens de auditoria são geradas no StorageGRID

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 as mensagens de auditoria específicas da API do S3.

As mensagens de auditoria são vinculadas por meio de identificadores específicos para cada protocolo.

Protocolo	Código
Vinculando operações S3	S3BK (bucket), S3KY (key) ou ambos
Interligação das operações internas	CBID (identificador interno do objeto)

Tempo das mensagens de auditoria

Devido a fatores como diferenças de tempo entre os nós da grade, tamanho do objeto e atrasos de rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar daquela mostrada nos exemplos desta seção.

Mensagens de auditoria para transações de ingest de objetos no StorageGRID

Você pode identificar as transações de ingestão do cliente no log de auditoria localizando as mensagens de auditoria específicas da API S3.

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão estão listadas na tabela a seguir. Apenas as mensagens necessárias para rastrear a transação de ingestão estão incluídas.

Mensagens de auditoria de ingestão S3

Código	Nome	Descrição	Rastrear	Ver
SPUT	Transação S3 PUT	Uma transação de ingestão S3 PUT foi concluída com sucesso.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras de objeto atendidas	A política ILM foi atendida para este objeto.	CBID	"ORLM: regras de objetos atendidas"

Exemplo: ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente ingere um objeto em um Storage Node (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM Make 2 Copies.

> Nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Apenas aquelas relacionadas à transação de ingestão no S3 (SPUT) estão listadas.

Este exemplo pressupõe que um bucket S3 já tenha sido criado.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação PUT do S3 foi emitida para criar um objeto em um bucket específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: regras de objetos atendidas

A mensagem ORLM indica que a política ILM foi atendida para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM que foi aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume dos locais dos objetos.

```
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 do bucket S3 e da chave.

```
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]]
```

Mensagens de auditoria para transações de exclusão de objetos no StorageGRID

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API S3.

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas nas tabelas a seguir. Somente as mensagens necessárias para rastrear a transação de exclusão estão incluídas.

Mensagens de auditoria de exclusão S3

Código	Nome	Descrição	Rastrear	Ver
SDEL	S3 Excluir	Solicitação feita para excluir o objeto de um bucket.	CBID, S3KY	"SDEL: S3 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 log de auditoria geradas durante uma transação de exclusão estão listadas no exemplo abaixo. Apenas aquelas relacionadas à transação de exclusão do S3 (SDEL) estão listadas.

SDEL: S3 Delete

A exclusão de objetos começa quando o cliente envia uma solicitação DeleteObject para um serviço LDR. A mensagem contém o bucket do qual o objeto será excluído e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Mensagens de auditoria para transações de recuperação de objetos no StorageGRID

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação estão listadas na tabela a seguir. Apenas as mensagens necessárias para rastrear a transação de recuperação estão incluídas.

Mensagens de auditoria de recuperação S3

Código	Nome	Descrição	Rastrear	Ver
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Exemplo: recuperação de objetos S3

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de

auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de log de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Apenas aquelas relacionadas à transação de recuperação do S3 (SGET) estão listadas.

SGET: S3 GET

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject a um serviço LDR. A mensagem contém o bucket do qual o objeto deve ser recuperado e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política do bucket permitir, um cliente pode recuperar objetos anonimamente ou recuperar objetos de um bucket pertencente a uma conta de tenant diferente. A mensagem de auditoria contém informações sobre a conta de tenant do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma solicitação GetObject para um objeto armazenado em um bucket que não lhe pertence. Os valores de SBAI e SBAC registram o ID e o nome da conta do locatário proprietário do bucket, que diferem do ID e do nome da conta do locatário do cliente registrados 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 Select em um objeto

Quando um cliente S3 executa uma consulta S3 Select em um objeto, mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Apenas aquelas relacionadas à transação S3 Select (SelectObjectContent) estão listadas.

Cada consulta resulta em duas mensagens de auditoria: uma que realiza a autorização da solicitação S3 Select (o campo S3SR é definido como "select") e uma operação GET padrão subsequente que recupera os dados do storage 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 auditoria para atualizações de metadados de objetos S3 no StorageGRID

As mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados S3

Código	Nome	Descrição	Rastrear	Ver
SUPD	Metadados S3 atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBID, S3KY, HTRH	"SUPD: Metadados S3 atualizados"

Exemplo: atualização de metadados do S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados (`x-amz-meta-*`) para o objeto S3 (S3KY). Neste exemplo, os cabeçalhos da solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (*Configuração* > **Monitoramento** > **Servidor de auditoria e syslog**). Consulte "Configurar o gerenciamento de logs e o servidor syslog externo".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Mensagens de auditoria

Saiba mais sobre os tipos e códigos de mensagens de auditoria no StorageGRID

As descrições detalhadas das mensagens de auditoria retornadas pelo sistema são apresentadas nas seções a seguir. Cada mensagem de auditoria é inicialmente listada em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades que são auditadas quanto para selecionar o tipo desejado de filtragem de

mensagens de auditoria.

As mensagens de auditoria também são listadas em ordem alfabética por seus códigos de quatro caracteres. Essa lista alfabética permite que você encontre informações sobre mensagens específicas.

Os códigos de quatro caracteres usados ao longo deste capítulo são os valores ATYP encontrados nas mensagens de auditoria, conforme mostrado na mensagem de exemplo a seguir:

```
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 os níveis de mensagens de auditoria, alterar os destinos de log e usar um servidor syslog externo para suas informações de auditoria, consulte "Configurar o gerenciamento de logs e o servidor syslog externo"

Categorias de mensagens de auditoria

Mensagens de auditoria para eventos do sistema no StorageGRID

As mensagens de auditoria pertencentes à categoria de auditoria do sistema são usadas para eventos relacionados ao próprio sistema de auditoria, estados dos nós da grade, atividade de tarefas em todo o sistema (tarefas da grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Ver
ECMC	Fragmento de dados codificado por apagamento ausente: indica que foi detectado um fragmento de dados codificado por apagamento ausente.	"ECMC: fragmento de dados codificado por apagamento ausente"
ECOC	Fragmento de dados codificado por apagamento corrompido: indica que um fragmento de dados codificado por apagamento corrompido foi detectado.	"ECOC: fragmento de dados codificado por apagamento corrompido"
ETAF	Falha na autenticação de segurança: uma tentativa de conexão usando Transport Layer Security (TLS) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: um serviço atualizou ou registrou informações sobre si mesmo no sistema StorageGRID.	"GNRG: Registro GNDS"
GNUR	Cancelamento de registro no GNDS: um serviço cancelou seu registro do sistema StorageGRID.	"GNUR: cancelamento do registro GNDS"

Código	Título e descrição da mensagem	Ver
GTED	Tarefa da grade finalizada: o serviço CMN concluiu o processamento da tarefa da grade.	"GTED: tarefa da grade concluída"
GTST	Tarefa da grade iniciada: o serviço CMN começou a processar a tarefa da grade.	"GTST: tarefa de grid iniciada"
GTSU	Tarefa de grade submetida: uma tarefa de grade foi submetida ao serviço CMN.	"GTSU: tarefa de grid enviada"
LLST	Localização perdida: Esta mensagem de auditoria é gerada quando uma localização é perdida.	"LLST: localização perdida"
OLST	Objeto perdido: um objeto solicitado não pode ser localizado no sistema StorageGRID.	"OLST: sistema detectou um objeto perdido."
SADD	Auditoria de segurança desativada: o registro de mensagens de auditoria foi desativado.	"SADD: desativar auditoria de segurança"
SADE	Auditoria de segurança ativada: o registro de mensagens de auditoria foi restaurado.	"SADE: habilitar auditoria de segurança"
SVRF	Falha na verificação do armazenamento de objetos: um bloco de conteúdo falhou nas verificações de integridade.	"SVRF: falha na verificação do armazenamento de objetos"
SVRU	Verificação do armazenamento de objetos desconhecido: dados de objeto inesperados detectados no armazenamento de objetos.	"SVRU: verificação de armazenamento de objetos desconhecida"
SYSD	Parada do nó: uma interrupção foi solicitada.	"SYSD: parada do nó"
SISTEMA	Parada do nó: um serviço iniciou uma parada controlada.	"SYST: Parada do nó"
SYSU	Início do nó: um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: início do nó"

Mensagens de auditoria para eventos de storage de objetos no StorageGRID

As mensagens de auditoria pertencentes à categoria de auditoria de storage de objetos são usadas para eventos relacionados ao armazenamento e gerenciamento de objetos dentro do sistema StorageGRID. Isso inclui storage de objetos e recuperações, transferências de nó da grade para nó da grade e verificações.

Os códigos de auditoria são removidos do produto e da documentação à medida que os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Mensagens de log de auditoria do storage de objetos StorageGRID 11.8".

Código	Descrição	Ver
BROR	Solicitação de somente leitura do bucket: um bucket entrou ou saiu do modo somente leitura.	"BROR: Solicitação de somente leitura do bucket"
CBSE	Fim do envio do objeto: a entidade de origem concluiu uma operação de transferência de dados de nó da grade para nó da grade.	"CBSE: Fim do envio de objeto"
CBRE	Fim do recebimento do objeto: A entidade de destino concluiu uma transferência de dados de nó da grade para nó da grade.	"CBRE: fim do recebimento de objeto"
CGRR	Solicitação de replicação entre grades: StorageGRID tentou uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grades.	"CGRR: Solicitação de Replicação entre Grids"
EBDL	Exclusão de bucket vazio: o scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de esvaziamento de bucket).	"EBDL: exclusão de bucket vazio"
EBKR	Solicitação de esvaziar o bucket: um usuário enviou uma solicitação para ativar ou desativar o esvaziamento do bucket (ou seja, para excluir objetos do bucket ou para interromper a exclusão de objetos).	"EBKR: Solicitação de bucket vazio"
SCMT	Confirmação do armazenamento de objetos: um bloco de conteúdo foi totalmente 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 da grade e não pode mais ser solicitado diretamente.	"SREM: Remover Object Store"

Mensagens de auditoria para operações de leitura do cliente no StorageGRID

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Ver
S3SL	Solicitação S3 Select: Registra uma conclusão 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: solicitação de seleção S3"
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 HEAD"

Mensagens de auditoria para operações de gravação do cliente no StorageGRID

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Ver
OVWR	Sobrescrita de objeto: registra uma transação para sobrescrever um objeto com outro objeto.	Cliente S3	"OVWR: sobrescrita de objeto"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou 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 AWS Glacier para um Cloud Storage Pool.	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	Metadados do S3 atualizados: registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	"SUPD: Metadados S3 atualizados"

Mensagens de auditoria de gerenciamento do StorageGRID

A categoria Gerenciamento registra as solicitações do usuário para a Management API.

Código	Título e descrição da mensagem	Ver
MGAU	Mensagem de auditoria da API de gerenciamento: um registro de solicitações do usuário.	"MGAU: mensagem de auditoria de gestão"

Mensagens de auditoria do StorageGRID ILM

As mensagens de auditoria pertencentes à categoria de auditoria ILM são usadas para eventos relacionados às operações de gerenciamento do ciclo de vida das informações (ILM).

Código	Título e descrição da mensagem	Ver
IDEL	Exclusão iniciada pelo ILM: esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
LKCU	Limpeza de Objeto Sobrescrito. Esta mensagem de auditoria é gerada quando um objeto sobrescrito é removido automaticamente para liberar espaço de storage.	"LKCU: Limpeza de objetos sobrescritos"
ORLM	Regras do objeto atendidas: Esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras do ILM.	"ORLM: regras de objetos atendidas"

Referência da mensagem de auditoria

Mensagem de log de auditoria BROR para solicitações somente leitura de bucket no StorageGRID

O serviço LDR gera esta mensagem de auditoria quando um bucket entra ou sai do modo somente leitura. Por exemplo, um bucket entra no modo somente leitura enquanto todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do bucket	O ID do bucket.
BROV	Valor da solicitação somente leitura do bucket	Indica se o bucket está sendo configurado como somente leitura ou se está deixando o estado de somente leitura (1 = somente leitura, 0 = não somente leitura).

Código	Campo	Descrição
BROS	Motivo de somente leitura do bucket	O motivo pelo qual o bucket está sendo definido como somente leitura ou saindo do estado somente leitura. Por exemplo, emptyBucket.
S3AI	ID da conta de locatário S3	O ID da conta do locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.

Mensagem de auditoria CBRB para início do recebimento de objeto no StorageGRID

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador único da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência do CBID foi iniciada por push ou por pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: a operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó de origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó de destino (receptor) da transferência CBID.
CTSS	Contagem inicial de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começará a partir dessa contagem de sequência.
CTES	Contagem esperada da sequência final	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência é considerada concluída quando essa contagem de sequência for recebida.

Código	Campo	Descrição
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi iniciada em um único conteúdo, identificado pelo seu Content Block Identifier. A operação solicita dados de "Start Sequence Count" até "Expected End Sequence Count". Os nós de envio e recebimento são identificados pelos seus node IDs. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar a contagem de réplicas.

Mensagem de auditoria CBRE para recebimento de objeto no StorageGRID

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador único da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência do CBID foi iniciada por push ou por pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: a operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó de origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó de destino (receptor) da transferência CBID.
CTSS	Contagem inicial de sequência	Indica a contagem sequencial em que a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequências transferida com sucesso. Se a Contagem Final de Sequências for igual à Contagem Inicial de Sequências e o Resultado da Transferência não tiver sido bem-sucedido, nenhum dado foi trocado.

Código	Campo	Descrição
RSLT	Resultado da transferência	Resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão excedido durante o estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados entre nós foi concluída. Se o resultado da transferência foi bem-sucedido, a operação transferiu dados de "Start Sequence Count" para "Actual End Sequence Count". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinada com mensagens de auditoria de armazenamento, também pode ser usada para verificar a contagem de réplicas.

Mensagem de auditoria CBSB para início do envio de objeto no StorageGRID

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador único da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência do CBID foi iniciada por push ou por pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: a operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó de origem (remetente) da transferência CBID.

Código	Campo	Descrição
CTDS	Entidade de destino	O ID do nó de destino (receptor) da transferência CBID.
CTSS	Contagem inicial de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começará a partir dessa contagem de sequência.
CTES	Contagem esperada da sequência final	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência é considerada concluída quando essa contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi iniciada em um único conteúdo, identificado pelo seu Content Block Identifier. A operação solicita dados de "Start Sequence Count" até "Expected End Sequence Count". Os nós de envio e recebimento são identificados pelos seus node IDs. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar a contagem de réplicas.

Mensagem de auditoria CBSE para o envio de objeto no StorageGRID

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador único da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência do CBID foi iniciada por push ou por pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: a operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó de origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó de destino (receptor) da transferência CBID.

Código	Campo	Descrição
CTSS	Contagem inicial de sequência	Indica a contagem sequencial em que a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequências transferida com sucesso. Se a Contagem Final de Sequências for igual à Contagem Inicial de Sequências e o Resultado da Transferência não tiver sido bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	Resultado da operação de transferência (da perspectiva da entidade remetente): SUCESSO: transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão excedido durante o estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados entre nós foi concluída. Se o resultado da transferência foi bem-sucedido, a operação transferiu dados de "Start Sequence Count" para "Actual End Sequence Count". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinada com mensagens de auditoria de armazenamento, também pode ser usada para verificar a contagem de réplicas.

Mensagem de auditoria CGRR para solicitações de replicação entre grades no StorageGRID

Esta mensagem é gerada quando o StorageGRID tenta uma operação de replicação entre grids para replicar objetos entre buckets em uma conexão de federação de grids.

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 grids que abrangem uma atualização do StorageGRID 11.7 para 11.8 podem apresentar um tamanho total de objeto impreciso.
S3AI	ID da conta de locatário S3	O ID da conta de locatário que possui o bucket do qual o objeto está sendo replicado.

Código	Campo	Descrição
GFID	ID de conexão da grid federation	O ID da conexão de federação de grid que está sendo usada para replicação entre grids.
OPER	Operação CGR	O tipo de operação de replicação entre grades que foi tentada: • 0 = Replicar objeto • 1 = Replicar objeto multipart • 2 = Replicar marcador de exclusão
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.
VSID	ID da versão	O ID da versão específica de um objeto que estava sendo replicado.
RSLT	Código de resultado	Retorna sucesso (SUCS) ou erro geral (GERR).

Mensagem de auditoria EBDL para exclusão de objetos de bucket vazio no StorageGRID

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de esvaziamento do bucket).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.
CAMINHO	Bucket/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner do objeto segmentado. Este valor está disponível somente se o objeto estiver segmentado.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
RSLT	Resultado da operação de exclusão	O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, usa-se NONE em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

Mensagem de log de auditoria EBKR para solicitações de bucket vazio no StorageGRID

Esta mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o

bucket vazio (ou seja, para excluir objetos do bucket ou para interromper a exclusão de objetos).

Código	Campo	Descrição
BUID	UUID do bucket	O ID do bucket.
EBJS	Configuração JSON de bucket vazio	Contém o JSON que representa a configuração atual do Empty Bucket.
S3AI	ID da conta de locatário S3	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.

Mensagem de log de auditoria ECMC para dados codificados de apagamento ausentes no StorageGRID

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados codificado por apagamento ausente.

Código	Campo	Descrição
VCMC	ID VCS	O nome do VCS que contém o chunk ausente.
MCID	ID do bloco	O identificador do fragmento codificado por apagamento ausente.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem em particular. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

Mensagem de auditoria ECOC para dados corrompidos com código de apagamento em StorageGRID

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados codificado por 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 por apagamento.
CCID	ID do bloco	O identificador do fragmento corrompido codificado por apagamento.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem em particular. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

Mensagem de auditoria ETAF para falhas de autenticação de segurança no StorageGRID

Esta mensagem é gerada quando uma tentativa de conexão usando o Transport Layer Security (TLS) falhou.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP na qual a autenticação falhou.
RUID	Identidade do usuário	Um identificador dependente do serviço que representa a identidade do usuário remoto.
RSLT	Código de motivo	O motivo da falha: SCNI: falha no estabelecimento da conexão segura. CERM: o certificado estava em falta. CERT: O certificado era inválido. CERE: o certificado expirou. CERR: O certificado foi revogado. CSGN: A assinatura do certificado era inválida. CSGU: o signatário do certificado era desconhecido. UCRM: As credenciais do usuário estavam ausentes. UCRI: As credenciais do usuário eram inválidas. UCRU: As credenciais do usuário foram recusadas. TOUT: Tempo limite de autenticação excedido.

Quando uma conexão é estabelecida com um serviço seguro que utiliza TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e lógica adicional integrada ao serviço. Se essa autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, uma mensagem de log de auditoria é registrada. Isso possibilita consultas sobre tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota com configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Essa mensagem de auditoria deve ser

monitorada para detectar tentativas de acesso não autorizado ao sistema.

Mensagem de auditoria GNRG para registro GNDS no StorageGRID

O serviço CMN gera esta mensagem de auditoria quando um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.
GNTP	Tipo de dispositivo	O tipo de dispositivo do nó da grid (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A string que identifica a versão do modelo do dispositivo do nó da grid no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consultas de serviço).
GNIA	Endereço IP	O endereço IP do nó de grid.

Esta mensagem é gerada sempre que um nó da grid atualiza sua entrada no Grid Nodes Bundle.

Mensagem de auditoria GNUR para cancelamento de registro GNDS no StorageGRID

O serviço CMN gera esta mensagem de auditoria quando um serviço removeu informações registradas sobre si mesmo 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 do nó	O ID do nó do serviço que iniciou a solicitação de atualização.

Mensagem de auditoria GTED para tarefas de grid finalizadas no StorageGRID

Esta mensagem de auditoria indica que o serviço CMN concluiu o processamento da tarefa de grid especificada e a moveu para a tabela Historical. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria correspondente de Grid Task Started. Os outros resultados indicam que o processamento desta tarefa de grid nunca foi iniciado.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grid gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Nota:** O ID da tarefa é atribuído no momento em que uma tarefa da grade é gerada, não no momento em que é submetida. É possível que uma determinada tarefa da grade seja submetida várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Submetida, Iniciada e Finalizada.
RSLT	Resultado	O resultado final do status da tarefa da grid: • SUCS: A tarefa na grade foi concluída com sucesso. • ABRT: A tarefa de grid foi encerrada sem um erro de reverter. • ROLF: A tarefa de grid foi encerrada e não foi possível concluir o processo de reverter. • CANC: A tarefa na grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa da grid expirou antes de ser iniciada. • IVLD: A tarefa da grid era inválida. • AUTENTICAÇÃO: a tarefa na grade não foi autorizada. • DUPL: A tarefa em grade foi rejeitada por ser duplicada.

Mensagem de log de auditoria GTST para tarefas de grid iniciadas no StorageGRID

Esta mensagem de auditoria indica que o serviço CMN iniciou o processamento da tarefa de grid especificada. A mensagem de auditoria é exibida imediatamente após a mensagem "Grid Task Submitted" para tarefas de grid iniciadas pelo serviço interno de Grid Task Submission e selecionadas para ativação automática. Para tarefas de grid submetidas na tabela Pending, esta mensagem é gerada quando o usuário inicia a tarefa de grid.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grid gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Nota:** O ID da tarefa é atribuído no momento em que uma tarefa da grade é gerada, não no momento em que é submetida. É possível que uma determinada tarefa da grade seja submetida várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Submetida, Iniciada e Finalizada.
RSLT	Resultado	O resultado. Este campo possui apenas um valor: • SUCS: A tarefa de grid foi iniciada com sucesso.

Mensagem de auditoria GTSU para tarefas de grid submetidas no StorageGRID

Esta mensagem de auditoria indica que uma tarefa de grid foi submetida ao serviço CMN.

Código	Campo	Descrição
TSID	ID da tarefa	Identifica de forma única uma tarefa de grid gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Nota:** O ID da tarefa é atribuído no momento em que uma tarefa da grade é gerada, não no momento em que é submetida. É possível que uma determinada tarefa da grade seja submetida várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Submetida, Iniciada e Finalizada.
TTYP	Tipo de tarefa	O tipo de tarefa em grade.
TVER	Versão da Tarefa	Um número que indica a versão da tarefa da grid.
TDSC	Descrição da tarefa	Uma descrição legível por humanos da tarefa da grade.
VATS	Válido após o carimbo de data/hora	O instante mais antigo (microssegundos UINT64 a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa da grid é válida.
VBTS	Válido antes do carimbo de data/hora	O horário mais recente (microssegundos UINT64 a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa da grid é válida.

Código	Campo	Descrição
TSRC	Fonte	A origem da tarefa: • TXTB: A tarefa de grid foi submetida através do sistema StorageGRID como um bloco de texto assinado. • GRID: A tarefa em grid foi enviada pelo Serviço Interno de Submissão de Tarefas do Grid.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa da grid foi submetida para ativação automática. • PENDENTE: A tarefa da grade foi submetida à tabela de pendências. Esta é a única possibilidade para a fonte TXTB.
RSLT	Resultado	O resultado da submissão: • SUCESSO: A tarefa em grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela de histórico.

Mensagem de auditoria IDEL para exclusões iniciadas pelo ILM no StorageGRID

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em 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 (presumindo que a configuração de exclusão automática esteja ativada e guarda legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis**. Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento nas políticas ILM ativas se aplica ao objeto.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CMPA	Conformidade: exclusão automática	Apenas para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o bucket esteja sob guarda legal.
CMPL	Conformidade: guarda legal	Apenas para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se o bucket está atualmente sob guarda legal.

Código	Campo	Descrição
CMPR	Conformidade: período de retenção	Apenas para objetos em buckets S3 compatíveis. O período de retenção do objeto em minutos.
CTME	Conformidade: tempo de ingestão	Apenas para objetos em buckets S3 compatíveis. O horário de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do bucket.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCS	Locais	Local de armazenamento dos dados do objeto dentro do sistema StorageGRID. O valor de LOCS é "" se o objeto não tiver locais (por exemplo, se tiver sido excluído). CLEC: para objetos com codificação de apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ID do nó ARC da localização do objeto, caso os dados do objeto estejam arquivados.
CAMINHO	Bucket/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	• Se um objeto em um bucket S3 compatível estiver sendo excluído automaticamente porque seu período de retenção expirou, este campo ficará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se aplicam atualmente ao objeto, este campo exibirá o rótulo legível da última regra ILM que foi aplicada ao objeto.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.

Código	Campo	Descrição
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de log de auditoria LKCU para limpeza de objeto sobrescrito no StorageGRID

Esta mensagem é gerada quando StorageGRID remove um objeto sobrescrito que anteriormente precisava ser limpo para liberar espaço de storage. Um objeto é sobrescrito quando um cliente S3 grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	*Apenas para uso interno.*
LUID	UUID do objeto removido	O identificador do objeto que foi removido.
CAMINHO	Bucket/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner do objeto segmentado. Este valor está disponível somente se o objeto estiver segmentado.
UUID	Identificador Único Universal	O identificador do objeto que ainda existe. Este valor só está disponível se o objeto não tiver sido excluído.

Mensagem de auditoria LKDM para limpeza de objeto vazado no StorageGRID

Esta mensagem é gerada quando um fragmento vazado é limpo ou excluído. Um fragmento pode fazer parte de um objeto replicado ou de um objeto codificado por apagamento.

Código	Campo	Descrição
CLOC	Localização do bloco	O caminho do arquivo do fragmento vazado que foi excluído.

Código	Campo	Descrição

CTYP	Tipo de bloco	Tipo de chunk:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	Tipo de vazamento	Os cinco tipos de vazamentos que podem ser detectados:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Tempo de criação de chunk	Hora em que o fragmento vazado foi criado.
UUID	Identificador Único Universal	O identificador do objeto ao qual o bloco pertence.
CBID	Identificador do bloco de conteúdo	CBID do objeto ao qual pertence o fragmento vazado.
CSIZ	Tamanho do conteúdo	O tamanho do bloco em bytes.

Mensagem de auditoria LLST para locais de cópia de objetos perdidos no StorageGRID

Esta mensagem é gerada sempre que não for possível encontrar a localização de uma cópia de um objeto (replicada ou codificada para apagamento).

Código	Campo	Descrição
CBIL	CBID	O CBID afetado.

Código	Campo	Descrição
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por apagamento. O ID do perfil de codificação por apagamento utilizado.
LTYP	Tipo de localização	CLDI (Online): para dados de objetos replicados CLEC (Online): para dados de objetos codificados por apagamento CLNL (Nearline): para dados de objetos replicados arquivados
NOID	ID do nó de origem	O ID do nó em que as localizações foram perdidas.
PCLD	Caminho para o objeto replicado	O caminho completo para a localização em disco dos dados do objeto perdido. Retornado somente quando LTYP tem o valor CLDI (ou seja, para objetos replicados). Assume a forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Resultado	Sempre NENHUM. RSLT é um campo obrigatório na mensagem, mas não é relevante para esta mensagem. NENHUM é usado em vez de SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de ativação	USUÁRIO: usuário acionou SYST: Sistema acionado
UUID	Identificador Único Universal	O identificador do objeto afetado no sistema StorageGRID.

Mensagem de auditoria MGAU para solicitações da API de gerenciamento no StorageGRID

A categoria Gerenciamento registra as solicitações de usuários para a Management API. Cada solicitação HTTP que não seja um método GET ou HEAD para um URI de API válido registra uma resposta contendo o nome de usuário, o endereço IP e o tipo de solicitação à API. URIs de API inválidos (como /api/v3-authorize) e solicitações inválidas para URIs de API válidos não são registradas.

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	Caminho da solicitação	O caminho da solicitação.
MPQP	Parâmetros de consulta da solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo da solicitação	O conteúdo do corpo da requisição. Embora o corpo da resposta seja registrado por padrão, o corpo da requisição é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo da resposta, elas são obtidas do corpo da requisição para os seguintes métodos POST: • Nome de usuário e ID da conta em **POST authorize** • Nova configuração de sub-redes em **POST /grid/grid-networks/update** • Novos servidores NTP em **POST /grid/ntp-servers/update** • IDs de servidores desativados em **POST /grid/servers/decommission** **Nota:** Informações sensíveis são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MRMD	Método de solicitação	O método de requisição HTTP: • POST • PUT • EXCLUIR • 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:** Informações sensíveis 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 do usuário	O URN (nome uniforme de recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna sucesso (SUCS) ou o erro relatado pelo backend.

Mensagem de auditoria OLST para objetos perdidos detectados pelo sistema no StorageGRID

Esta mensagem é gerada quando o serviço DDS não consegue localizar nenhuma cópia de um objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto perdido.
NOID	ID do nó	Se disponível, a última localização direta ou próxima conhecida do objeto perdido. É possível ter apenas o ID do nó sem o ID do volume, caso as informações de volume não estejam disponíveis.
CAMINHO	Bucket/Chave S3	Se disponíveis, o nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez de SUCS para que esta mensagem não seja filtrada.
UUID	Identificador Único Universal	O identificador do objeto perdido dentro do sistema StorageGRID.
VOLI	ID do volume	Se disponível, o ID do volume do Storage Node correspondente à última localização conhecida do objeto perdido.

Mensagem de auditoria ORLM para regras ILM atendidas no StorageGRID

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras do ILM.

> ⓘ A mensagem ORLM não é gerada quando um objeto é armazenado com sucesso pela regra padrão Make 2 Copies se outra regra na política usar o filtro avançado Object Size.

Código	Campo	Descrição
BUID	Cabeçalho de bucket	Campo ID do bucket. Usado para operações internas. Aparece somente 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
LOCS	Locais	Local de armazenamento dos dados do objeto dentro do sistema StorageGRID. O valor de LOCS é "" se o objeto não tiver locais (por exemplo, se tiver sido excluído). CLEC: para objetos com codificação de apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ID do nó ARC da localização do objeto, caso os dados do objeto estejam arquivados.
CAMINHO	Bucket/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível por humanos atribuído à regra ILM aplicada a este objeto.
SEGC	UUID do contêiner	UUID do contêiner do objeto segmentado. Este valor está disponível somente se o objeto estiver segmentado.
SGCB	Contêiner CBID	CBID do contêiner do objeto segmentado. Este valor está disponível apenas para objetos segmentados e multipartes.
ESTAT	Status	O status da operação do ILM. CONCLUÍDO: as operações ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação do ILM. PRGD: O objeto foi excluído do sistema StorageGRID. NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID. Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

A mensagem de auditoria ORLM pode ser emitida mais de uma vez para um único objeto. Por exemplo, ela é emitida sempre que um dos seguintes eventos ocorre:

- As regras ILM para o objeto são satisfeitas para sempre.
- As regras ILM para o objeto foram atendidas neste epoch.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano detecta que uma cópia dos dados de um objeto replicado está corrompida. O sistema StorageGRID realiza uma avaliação ILM para substituir o objeto corrompido.

Informações relacionadas

- "Transações de ingestão de objetos"
- "Transações de exclusão de objetos"

Mensagem de auditoria OVWR para sobrescritas de objetos no StorageGRID

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja sobrescrito por outro objeto.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo (novo)	O CBID do novo objeto.
CSIZ	Tamanho do objeto anterior	O tamanho, em bytes, do objeto que está sendo sobrescrito.
OCBD	Identificador do bloco de conteúdo (anterior)	O CBID do objeto anterior.
UUID	Identificação Única Universal (new)	O identificador do novo objeto dentro do sistema StorageGRID.
OUID	Identificação Única Universal (anterior)	O identificador do objeto anterior dentro do sistema StorageGRID.
CAMINHO	Caminho do objeto S3	O caminho do objeto S3 usado tanto para o objeto anterior quanto para o novo objeto
RSLT	Código de resultado	Resultado da transação de sobrescrita de objeto. O resultado é sempre: SUCS: Bem-sucedido
SGRP	Site (Grupo)	Caso presente, o objeto sobrescrito foi excluído no site especificado, que não é o site onde o objeto sobrescrito foi ingerido.

Mensagem de auditoria S3SL para solicitações S3 Select no StorageGRID

Esta mensagem registra a conclusão de uma solicitação S3 Select que foi retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.

Código	Campo	Descrição
BYSC	Bytes verificados	Número de bytes verificados (recebidos) dos nós de armazenamento. BYSC e BYPR provavelmente serão diferentes se o objeto estiver compactado. Se o objeto estiver compactado, BYSC conterá a contagem de bytes compactados e BYPR conterá os bytes após a descompactação.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "Bytes Scanned" foram realmente processados ou utilizados por uma tarefa S3 Select.
BYRT	Bytes retornados	Número de bytes que uma tarefa S3 Select retornou ao cliente.
REPR	Registros processados	Número de registros ou linhas que uma tarefa S3 Select recebeu dos nós de armazenamento.
RERT	Registros retornados	Número de registros ou linhas que um trabalho S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se a tarefa de seleção do S3 terminou o processamento ou não. Se for falso, a tarefa não foi concluída e os campos de erro provavelmente conterão dados. O cliente pode ter recebido resultados parciais ou nenhum resultado.
REID	ID da solicitação	Identificador da solicitação S3 Select.
EXTM	Tempo de execução	O tempo, em segundos, que a tarefa S3 Select Job levou para ser concluída.
ERMG	Mensagem de erro	Mensagem de erro que a tarefa S3 Select gerou.
ERTY	Tipo de erro	Tipo de erro que a tarefa S3 Select gerou.
ERST	Rastreamento de pilha de erros	Rastreamento de pilha de erros que a tarefa S3 Select gerou.
S3BK	Bucket S3	O nome do bucket S3.

Código	Campo	Descrição
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 do usuário que enviou a solicitação.
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do tenant do usuário que enviou a solicitação.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.

Mensagem de auditoria SADD para desativação da auditoria de segurança no StorageGRID

Esta mensagem indica que o serviço de origem (ID do nó) desativou o registro de mensagens de auditoria. StorageGRID não está mais coletando nem entregando mensagens de auditoria.

Código	Campo	Descrição
AETM	Habilitar método	O método utilizado para desativar a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para desativar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro de logs estava previamente ativado, mas agora foi desativado. 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 (SADE) e a capacidade de desativar a auditoria é então bloqueada permanentemente.

Mensagem de auditoria SADE para ativação da auditoria de segurança no StorageGRID

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registro de mensagens de auditoria. StorageGRID está novamente coletando e entregando mensagens de auditoria.

Código	Campo	Descrição
AETM	Habilitar método	O método utilizado para habilitar a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para ativar o registro de auditoria.

Código	Campo	Descrição
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 indica que o registro de logs estava desativado anteriormente (SADD), mas agora foi 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 bloqueada permanentemente.

Mensagem de auditoria SCMT para commits de armazenamento de objetos no StorageGRID

O conteúdo da grade não é disponibilizado ou reconhecido como armazenado até que seja confirmado (ou seja, armazenado de forma persistente). O conteúdo armazenado de forma persistente foi completamente gravado em disco e passou pelas verificações de integridade pertinentes. Esta mensagem é emitida quando um bloco de conteúdo é confirmado no armazenamento.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo gravado no armazenamento permanente.
RSLT	Código de resultado	Status no momento em que o objeto foi armazenado em disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi totalmente armazenado e verificado, e agora pode ser solicitado. Ela pode ser usada para rastrear o fluxo de dados dentro do sistema.

Mensagem de auditoria SDEL para transações DELETE do S3 no StorageGRID

Quando um cliente S3 emite uma transação DELETE, é feita uma solicitação para remover o objeto ou bucket especificado, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em buckets não incluem este campo.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
GFID	ID de conexão da Grid Federation	O ID de conexão da federação de grids associada a uma solicitação de exclusão de replicação entre grids. Incluído apenas nos logs de auditoria no grid de destino.
GFSA	ID da conta de origem da Grid Federation	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grades. Incluído apenas nos logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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	Última hora de modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.

Código	Campo	Descrição
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
S3SR	Subrecurso S3	O bucket ou subrecurso de objeto em que a operação está sendo realizada, se aplicável.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.

Código	Campo	Descrição
UUDM	Identificador universalmente único para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens de log de auditoria especificam UUDM ou UUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto e UUID indica um objeto.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de auditoria SGET para transações GET do S3 no StorageGRID

Quando um cliente S3 emite uma transação GET, é feita uma solicitação para recuperar um objeto, listar os objetos em um bucket ou remover um bucket/subrecurso de objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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).

Código	Campo	Descrição
LITY	ListObjectsV2	Foi solicitada uma resposta no formato *v2*. Para detalhes, veja "AWS ListObjectsV2". Apenas para operações GET em bucket.
NCHD	Número de filhos	Inclui chaves e prefixos comuns. Somente para operações GET em buckets.
ALCANCE	Leitura de intervalo	Apenas para operações de leitura de intervalo. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho do objeto inteiro.
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
S3SR	Subrecurso S3	O bucket ou subrecurso de objeto em que a operação está sendo realizada, se aplicável.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.

Código	Campo	Descrição
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.
TRNC	Truncado ou não truncado	Defina como falso se todos os resultados forem retornados. Defina como verdadeiro se houver mais resultados disponíveis para retornar. Somente para operações GET no bucket.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de auditoria SHEA para operações S3 HEAD no StorageGRID

Quando um cliente S3 emite uma operação HEAD, é feita uma solicitação para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a operação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. Operações em buckets não incluem este campo.
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto selecionado em bytes. Operações em buckets não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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 de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.

Código	Campo	Descrição
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de auditoria SPOS para transações POST do S3 no StorageGRID

Quando um cliente S3 emite uma solicitação POST Object, esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único 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 presente na solicitação.
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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 de resultado	Resultado da solicitação RestoreObject. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
S3SR	Subrecurso S3	O bucket ou subrecurso de objeto em que a operação está sendo realizada, se aplicável. Defina como "select" para uma operação S3 Select.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SRCF	Configuração de subresource	Restaurar informações.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de auditoria SPUT para transações PUT do S3 no StorageGRID

Quando um cliente S3 emite uma transação PUT, é feita uma solicitação para criar um novo objeto ou bucket, ou para remover um bucket/subrecurso de objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. Operações em buckets não incluem este campo.
CMPS	Configurações de conformidade	As configurações de conformidade usadas ao criar o bucket, se presentes na solicitação (truncadas para os primeiros 1024 caracteres).

Código	Campo	Descrição
CNCH	Cabeçalho de controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
GFID	ID de conexão da Grid Federation	O ID de conexão da federação de grids associada a uma solicitação PUT de replicação entre grids. Incluído apenas nos logs de auditoria no grid de destino.
GFSA	ID da conta de origem da Grid Federation	O ID da conta do locatário na grade de origem para uma solicitação PUT de replicação entre grades. Incluído apenas nos logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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 de objeto ativado	Valor do cabeçalho da requisição `x-amz-bucket-object-lock-enabled`, se presente na requisição.
LKLH	Bloqueio de Objeto Retenção Legal	Valor do cabeçalho da requisição `x-amz-object-lock-legal-hold`, se presente na requisição PutObject.
LKMD	Modo de retenção de bloqueio de objeto	Valor do cabeçalho da requisição `x-amz-object-lock-mode`, se presente na requisição PutObject.

Código	Campo	Descrição
LKRU	Reter objeto até a data	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date`, se presente na solicitação PutObject. Os valores são limitados a um período de 100 anos a partir da data em que o objeto foi ingerido.
MTME	Última hora de modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
S3SR	Subrecurso S3	O bucket ou subrecurso de objeto em que a operação está sendo realizada, se aplicável.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.

Código	Campo	Descrição
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SRCF	Configuração de subresource	A nova configuração do subrecurso (truncada para os primeiros 1024 caracteres).
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.
ULID	ID de upload	Incluído apenas nas mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as partes foram carregadas e montadas.
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de versionamento	O novo estado de versionamento de um bucket. Dois estados são usados: "ativado" ou "suspenso". Operações em objetos não incluem este campo.

Mensagem de auditoria SREM para remoção de armazenamento de objetos no StorageGRID

Esta mensagem é emitida quando o conteúdo é removido do storage persistente e deixa de estar acessível através das APIs regulares.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo excluído do storage permanente.

Código	Campo	Descrição
RSLT	Código de resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do storage persistente

Esta mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

Mensagem de auditoria SUPD para atualizações de metadados S3 no StorageGRID

Esta mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização dos metadados for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de conexão	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista dos nomes e valores dos cabeçalhos de requisição 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 de resultado	Resultado da transação GET. O resultado é sempre: SUCS: bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 criptografado para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Bucket S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. As operações em buckets não incluem este campo.
SACC	Nome da conta do tenant S3 (remetente da solicitação)	Nome da conta de locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do tenant S3 (proprietário do bucket)	Nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou acesso anônimo.
SBAI	ID da conta do tenant S3 (proprietário do bucket)	O ID da conta do locatário proprietário do bucket de destino. Usado para identificar acesso entre contas ou acesso anônimo.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que está fazendo a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Deixe em branco para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga de camada 7 confiável, o endereço IP do balanceador de carga.

Código	Campo	Descrição
UUID	Identificador Único Universal	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

Mensagem de auditoria SVRF para falhas de verificação de armazenamento de objetos no StorageGRID

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que dados de objetos replicados são lidos ou gravados em disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente inseridos no sistema. Se alguma dessas verificações falhar, o sistema automaticamente coloca em quarentena os dados corrompidos do objeto replicado para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador único do bloco de conteúdo cuja verificação falhou.
RSLT	Código de resultado	Tipo de falha na verificação: CRCF: verificação de redundância cíclica (CRC) falhou. HMAC: a verificação do código de autenticação de mensagem baseado em hash (HMAC) falhou. EHSH: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. ERRO: Estrutura de arquivo de disco inválida. DERR: Erro de disco. FNAM: Nome de arquivo inválido.

Esta mensagem deve ser monitorada atentamente. Falhas na verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar qual operação gerou a mensagem, verifique o valor do campo AMID (ID do Módulo). Por exemplo, o 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 gerada pela recuperação de conteúdo.

Mensagem de auditoria SVRU para conteúdo de armazenamento de objetos desconhecido no StorageGRID

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detectada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do arquivo	O caminho do arquivo da cópia inesperada do objeto.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

> A mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada atentamente. Ela significa que cópias inesperadas de dados de objetos foram detectadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar falhas de hardware iminentes.

Mensagem de auditoria SYSD para paradas controladas de nós no StorageGRID

Quando um serviço é encerrado normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, esta mensagem é enviada somente após um reiniciar, pois a fila de mensagens de auditoria não é limpa antes do desligamento. Procure pela mensagem SYST, enviada no início da sequência de desligamento, caso o serviço não tenha sido reiniciado.

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza da paralisação: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatório. O RSLT de um SYSD não pode indicar um desligamento "sujo", pois a mensagem é gerada apenas por desligamentos "limpos".

Mensagem de auditoria SYST para nó parando no StorageGRID

Quando um serviço é encerrado corretamente, esta mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. SYST pode ser usado para determinar se o desligamento foi solicitado antes que o serviço seja reiniciado (diferentemente de SYSD, que normalmente é enviado após o serviço ser reiniciado).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza da paralisação: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatório. O código RSLT de uma mensagem SYST não pode indicar um desligamento "sujo", pois a mensagem é gerada apenas por desligamentos "limpos".

Mensagem de auditoria SYSU para nó inicia no StorageGRID

Quando um serviço é reiniciado, esta mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza da paralisação: SUCS: O sistema foi desligado corretamente. DSDN: o sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação (ou reinstalação) do servidor.

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatório. Esta mensagem pode ser usada para:

- Detectar descontinuidades no log de auditoria.
- Determine se um serviço está apresentando falhas durante a operação (já que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). Server Manager reinicia automaticamente o serviço com falha.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

Informações sobre marcas comerciais

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