



Monitore o sistema StorageGRID

StorageGRID

NetApp
November 04, 2025

Índice

Monitore o sistema StorageGRID	1
Monitorar um sistema StorageGRID: Visão geral	1
Visualizar e gerenciar o painel	1
Visualizar o painel de instrumentos	2
Gerenciar painéis	3
Configurar painéis	4
Exibir a página nós	4
Exibir a página de nós: Visão geral	4
Veja a guia Visão geral	7
Exibir a guia hardware	9
Veja a guia rede	26
Exibir a guia armazenamento	27
Exibir a guia objetos	29
Veja a guia ILM	31
Use a guia tarefas	32
Veja a guia balanceador de carga	32
Veja a guia Serviços da Plataforma	34
Exibir a guia Gerenciar unidades (somente SGF6112)	35
Exibir a guia Gerenciador de sistema do SANtricity (somente Série e)	36
Informações para monitorar regularmente	38
O que e quando monitorar	38
Monitorar a integridade do sistema	39
Monitorar a capacidade de armazenamento	43
Monitorar o gerenciamento do ciclo de vida das informações	51
Monitorar recursos de rede e do sistema	52
Monitorar a atividade do locatário	56
Monitore as operações dos clientes S3 e Swift	61
Monitorar operações de balanceamento de carga	62
Monitorar conexões de federação de grade	63
Monitorar a capacidade de arquivamento	68
Alertas e alarmes	68
Gerenciar alertas e alarmes: Visão geral	69
Compare alertas e alarmes	69
Gerenciar alertas	73
Referência de alertas	93
Métricas de Prometheus comumente usadas	106
Gerenciar alarmes (sistema legado)	111
Referência de alarmes (sistema legado)	133
Referência de ficheiros de registo	162
Referência de ficheiros de registo: Visão geral	162
Registos do software StorageGRID	164
Logs de implantação e manutenção	170
Logs para software de terceiros	171

Sobre o bycast.log	172
Configurar destinos de mensagens de auditoria e de log	181
Considerações para usar um servidor syslog externo	181
Configurar mensagens de auditoria e servidor syslog externo	186
Utilize a monitorização SNMP	195
Usar monitoramento SNMP: Visão geral	195
Configure o agente SNMP	197
Atualize o agente SNMP	204
Acesse arquivos MIB	205
Colete dados adicionais do StorageGRID	207
Use gráficos e gráficos	207
Use relatórios de texto	219
Monitore O PUT e obtenha desempenho	223
Monitorar operações de verificação de objetos	224
Monitorar eventos	226
Rever mensagens de auditoria	230
Colete arquivos de log e dados do sistema	231
Acione manualmente um pacote AutoSupport	233
Veja a árvore de topologia de Grade	234
Analise as métricas de suporte	235
Execute o diagnóstico	237
Crie aplicativos de monitoramento personalizados	241

Monitore o sistema StorageGRID

Monitorar um sistema StorageGRID: Visão geral

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

Antes de começar

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



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

Sobre esta tarefa

Estas instruções descrevem como:

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

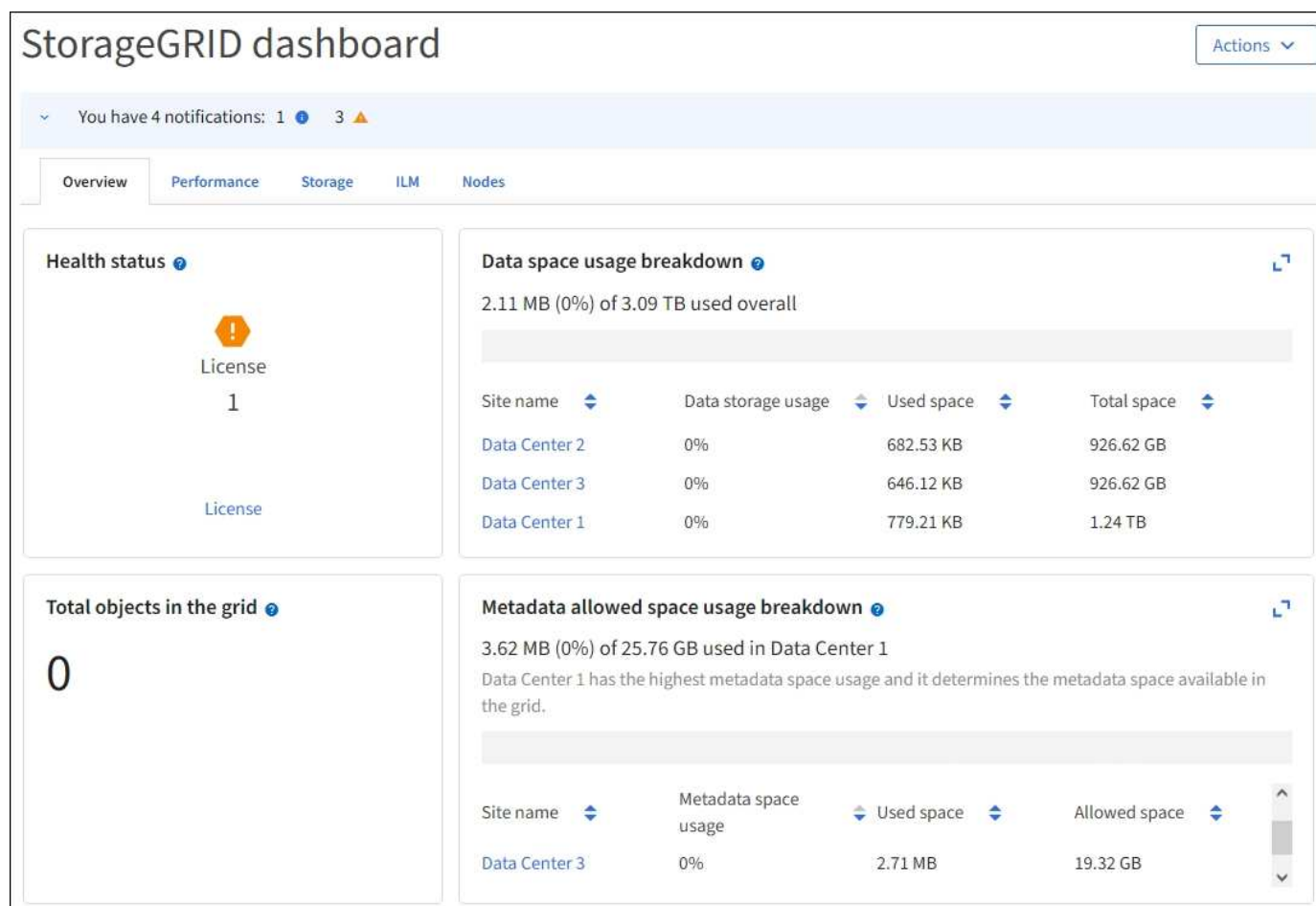
Visualizar e gerenciar o painel

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



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

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



Visualizar o painel de instrumentos



O painel é composto por separadores que contêm informações específicas sobre o sistema StorageGRID. Cada guia contém categorias de informações exibidas nos cartões.

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

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

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

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

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

Gerenciar painéis

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

- Crie um painel personalizado do zero. Você pode usar painéis personalizados para controlar quais informações do StorageGRID são exibidas e como essas informações são organizadas.
- Clonar um painel para criar painéis personalizados.
- Defina um painel ativo para um usuário. O painel ativo pode ser o painel fornecido pelo sistema ou um painel personalizado.
- Defina um painel padrão, que é o que todos os usuários veem, a menos que ativem seu próprio painel.
- Edite um nome de painel.
- Edite um painel para adicionar ou remover guias e cartões. Você pode ter um mínimo de 1 e um máximo de 20 guias.
- Retire um painel de bordo.



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

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



Configurar painéis

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

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



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

Ao configurar um dashboard, você pode:

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

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Exibir a página nós

Exibir a página de nós: Visão geral

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

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






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



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



Nodes

View the list and status of sites and grid nodes.

Search...					Total node count: 12
Name	Type	Object data used	Object metadata used	CPU usage	
StorageGRID Webscale Deployment	Grid	0%	0%	—	
^ DC1	Site	0%	0%	—	
 DC1-ADM1	Primary Admin Node	—	—	6%	
 DC1-ARC1	Archive Node	—	—	1%	
 DC1-G1	Gateway Node	—	—	3%	
DC1-S1	Storage Node	0%	0%	6%	
DC1-S2	Storage Node	0%	0%	8%	
DC1-S3	Storage Node	0%	0%	4%	

Ícones de estado da ligação


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


Ícone	Descrição	Ação necessária
	<p>Não ligado - desconhecido</p> <p>Por um motivo desconhecido, um nó é desconetado ou os serviços no nó estão inalterados inesperadamente. Por exemplo, um serviço no nó pode ser interrompido ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada.</p> <p>O alerta não é possível se comunicar com o nó também pode ser acionado. Outros alertas também podem estar ativos.</p>	<p>Requer atenção imediata. "Selecione cada alerta" e siga as ações recomendadas.</p> <p>Por exemplo, talvez seja necessário reiniciar um serviço que tenha parado ou reiniciado o host para o nó.</p> <p>Nota: Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.</p>
	<p>Não conectado - administrativamente para baixo</p> <p>Por um motivo esperado, o nó não está conectado à grade.</p> <p>Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.</p> <p>Com base no problema subjacente, esses nós geralmente voltam online sem nenhuma intervenção.</p>	<p>Determine se algum alerta está afetando esse nó.</p> <p>Se um ou mais alertas estiverem ativos "Selecione cada alerta" e siga as ações recomendadas.</p>


Se um nó for desconetado da grade, ele pode ter um alerta subjacente, mas somente o ícone "não conectado" será exibido. Para ver os alertas ativos de um nó, selecione o nó.

Ícones de alerta

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

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

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

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

Exibir detalhes de um sistema, local ou nó

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

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

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

Veja a guia Visão geral

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

A guia Visão geral é mostrada para todos os nós.



Informações do nó

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

NYC-ADM1 (Primary Admin Node)

Overview Hardware Network Storage Load balancer Tasks

Node information




Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	 Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)
	Show additional IP addresses 

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

- **Nome de exibição** (mostrado somente se o nó tiver sido renomeado): O nome de exibição atual do nó. Utilize o ["Renomeie grade, sites e nós"](#) procedimento para atualizar este valor.
- **Nome do sistema**: O nome que você inseriu para o nó durante a instalação. Os nomes do sistema são usados para operações internas do StorageGRID e não podem ser alterados.
- **Tipo**: O tipo de nó — nó Admin, nó Admin primário, nó de armazenamento, nó de gateway ou nó de arquivo.



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

- **ID**: O identificador exclusivo para o nó, que também é conhecido como UUID.
- **Estado da conexão**: Um dos três estados. É apresentado o ícone para o estado mais grave.
 - **Desconhecido** : por um motivo desconhecido, o nó não está conectado à grade ou um ou mais serviços estão inalterados inesperadamente. Por exemplo, a conexão de rede entre nós foi perdida, a energia está inativa ou um serviço está inativo. O alerta **não é possível se comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.
- **Administrativamente para baixo** : o nó não está conectado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.
- **Conectado** : o nó está conectado à grade.
- **Storage usado**: Somente para nós de storage.
 - **Dados do objeto**: A porcentagem do espaço utilizável total para dados de objeto que foram usados no nó de armazenamento.
 - **Metadados de objetos**: A porcentagem do espaço total permitido para metadados de objetos que foram usados no nó de armazenamento.
- **Versão do software**: A versão do StorageGRID instalada no nó.
- **Grupos de HA**: Somente para nó de administrador e nós de gateway. Mostrado se uma interface de rede no nó está incluída em um grupo de alta disponibilidade e se essa interface é a interface principal.
- **Endereços IP**: Os endereços IP do nó. Clique em **Mostrar endereços IP adicionais** para visualizar os endereços IPv4 e IPv6 do nó e mapeamentos de interface.

Alertas

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

Alerts			
Alert name	Severity	Time triggered	Current values
Low installed node memory The amount of installed memory on a node is low.	✖ Critical	11 hours ago	Total RAM size: 8.37 GB

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

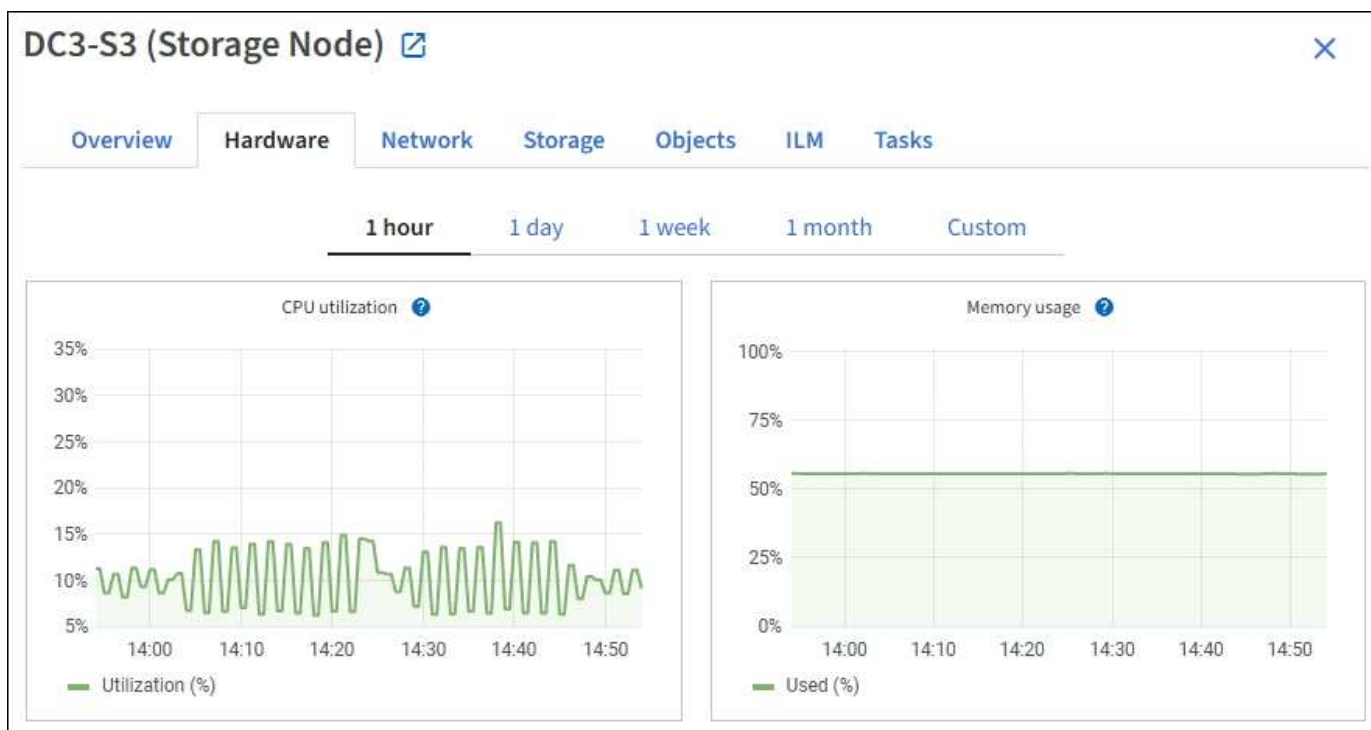
Exibir a guia hardware

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



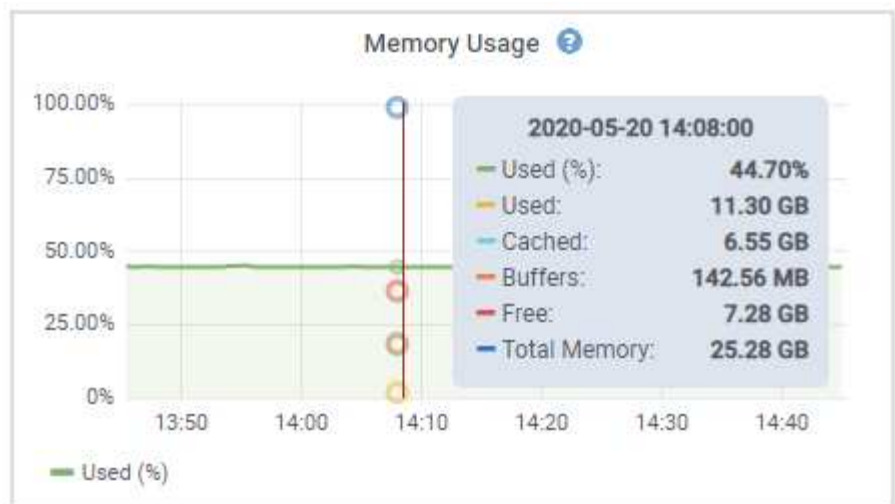
O Gerenciador de Grade é atualizado com cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A guia hardware é exibida para todos os nós.



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

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



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

Exibir informações sobre os nós de storage do dispositivo

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

Passos

1. Na página nós, selecione um nó de storage do dispositivo.
2. Selecione **Visão geral**.

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

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

DC2-SGA-010-096-106-021 (Storage Node) [↗](#)



Overview

Hardware

Network

Storage

Objects

ILM

Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state: Connected

Storage used: Object data 7% [?](#)
Object metadata 5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ^	IP address ^
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

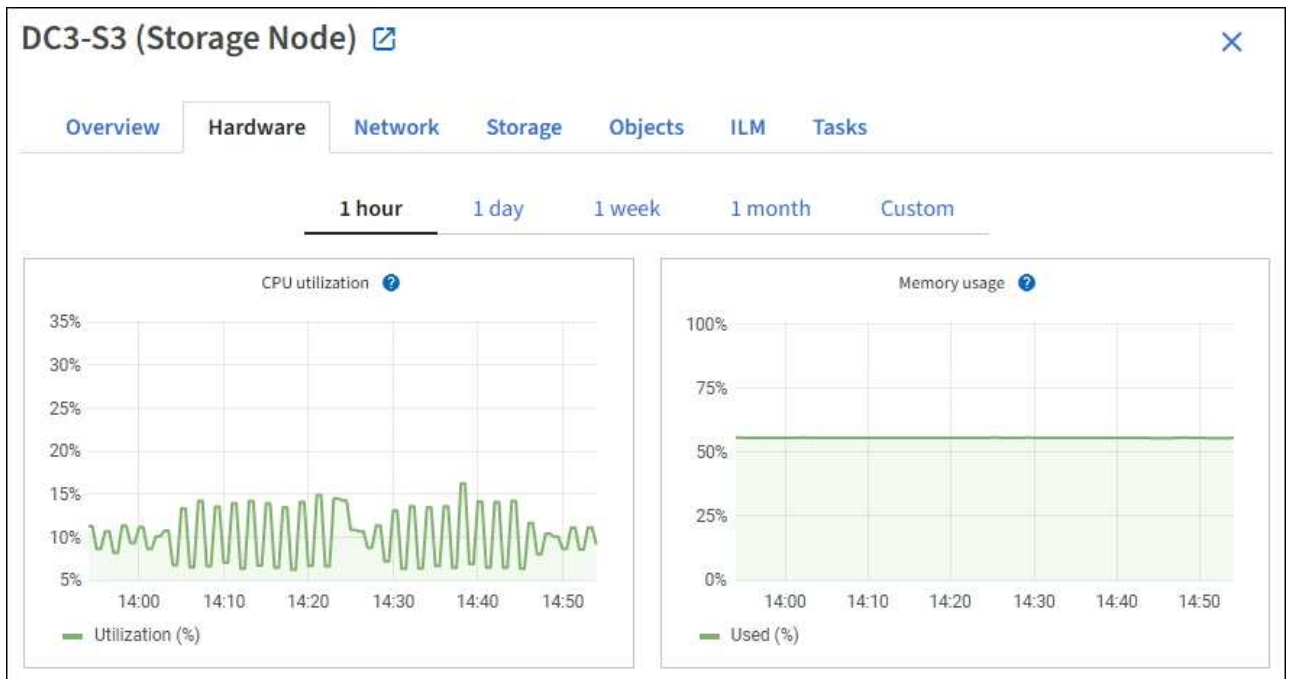
Alerts

Alert name ^	Severity ? ^	Time triggered ^	Current values
ILM placement unachievable ↗	Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

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

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

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






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



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

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

StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

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

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

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

+

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

Coluna na tabela prateleiras de armazenamento	Descrição
ID do compartimento	<p>O identificador numérico da prateleira de armazenamento.</p> <ul style="list-style-type: none"> • 99: Compartimento do controlador de storage • 0: Primeira prateleira de expansão • 1: Segunda prateleira de expansão <p>Nota: as prateleiras de expansão aplicam-se apenas aos modelos SG6060 e SG6160.</p>
Status do compartimento	O status geral da gaveta de storage.
Estado IOM	O status dos módulos de entrada/saída (IOMs) em quaisquer prateleiras de expansão. N/A se este não for um compartimento de expansão.
Estado da fonte de alimentação	O status geral das fontes de alimentação para o compartimento de armazenamento.
Estado da gaveta	O estado das gavetas na prateleira de arrumação. N/A se a prateleira não contiver gavetas.
Estado da ventoinha	O status geral dos ventiladores de resfriamento na prateleira de armazenamento.
Slots de unidade	O número total de slots de unidade no compartimento de armazenamento.
Unidades de dados	O número de unidades no compartimento de storage usadas para o storage de dados.
tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados no compartimento de storage.
Unidades de cache	O número de unidades no compartimento de armazenamento que são usadas como cache.
Tamanho da unidade de cache	O tamanho da menor unidade de cache no compartimento de armazenamento. Normalmente, as unidades de cache têm o mesmo tamanho.
Estado da configuração	O status de configuração do compartimento de storage.

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

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

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

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

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



a. Reveja a secção interfaces de rede.

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

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



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

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

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

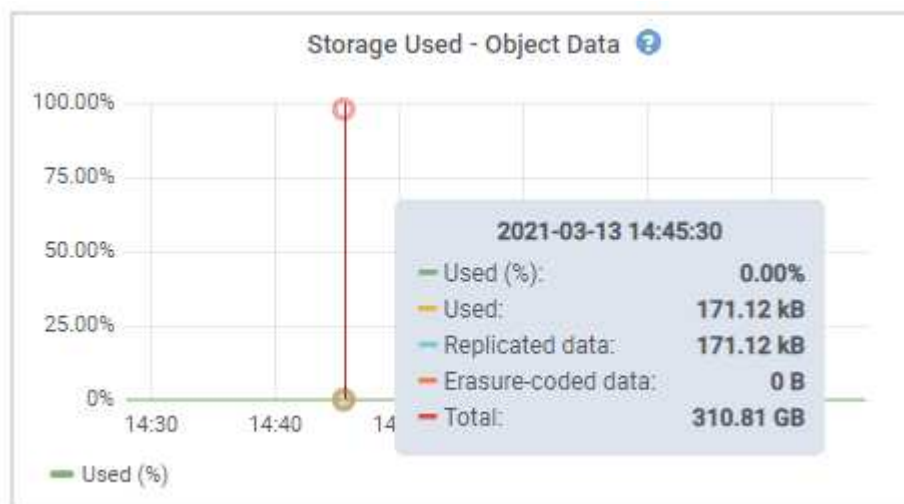
Consulte "[Configurar ligações de rede](#)" para obter mais informações sobre como configurar as portas 10/25-GbE.

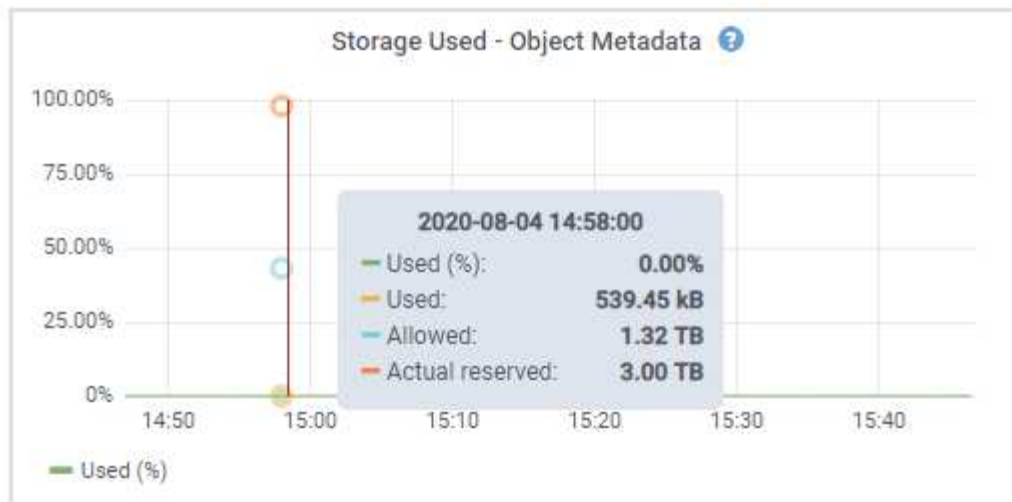
b. Reveja a secção Comunicação de rede.

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

Network communication						
Receive						
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

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





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






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

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

Disk devices

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

Volumes

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

Object stores

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

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

A página nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada dispositivo de serviços que é usado como nó de administrador ou nó de gateway. Você também pode ver memória, hardware de armazenamento, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

Passos

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

A seção informações do nó da guia Visão geral exibe informações resumidas do nó, como nome, tipo, ID e

estado da conexão do nó. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte forma:

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

10-224-6-199-ADM1 (Primary Admin Node) [🔗](#) [✕](#)

Overview

Hardware

Network

Storage

Load balancer

Tasks

SANtricity System Manager

Node information [?](#)

Name:

10-224-6-199-ADM1

Type:

Primary Admin Node

ID:

6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:

✔

Connected

Software version:

11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

172.16.6.199 - eth0 (Grid Network)

10.224.6.199 - eth1 (Admin Network)

47.47.7.241 - eth2 (Client Network)

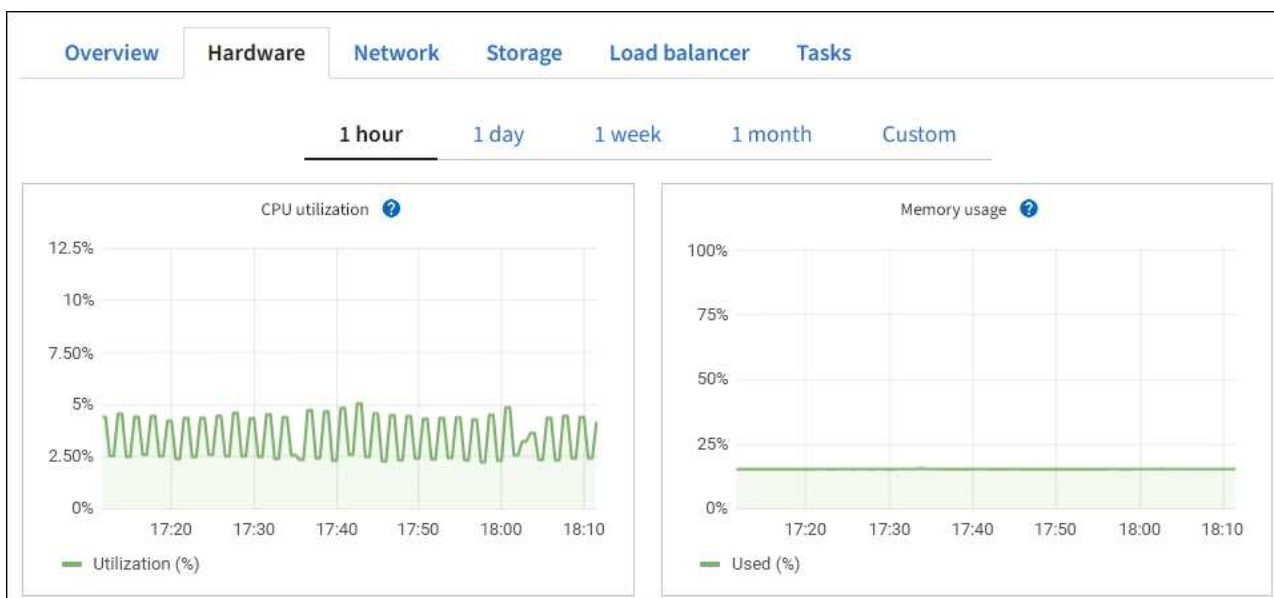
[Hide additional IP addresses ^](#)

Interface ↕	IP address ↕
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

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

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

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



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

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

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

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

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

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

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

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



a. Reveja a secção interfaces de rede.

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

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



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

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

b. Reveja a secção Comunicação de rede.

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

Network communication

Receive

Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit



Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

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

Disk devices

Name ? ⬆️⬆️	World Wide Name ? ⬆️⬆️	I/O load ? ⬆️⬆️	Read rate ? ⬆️⬆️	Write rate ? ⬆️⬆️
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 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	84.63 GB 	Unknown

Veja a guia rede

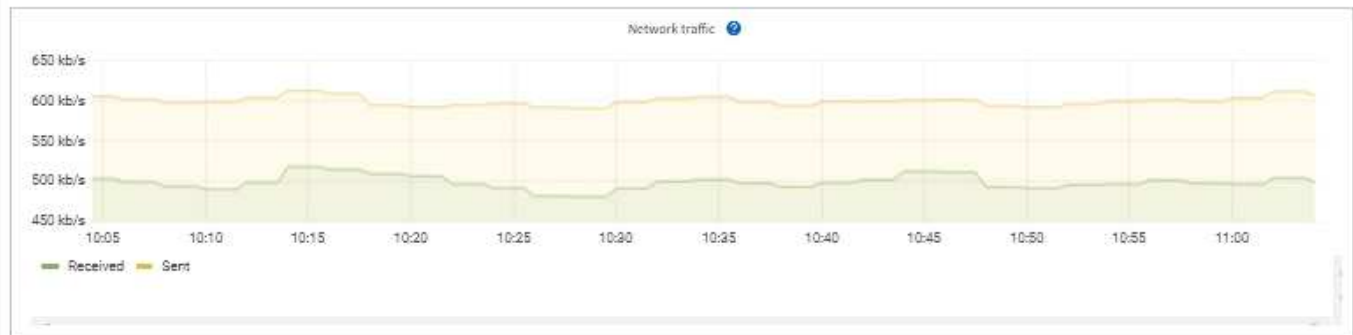
A guia rede exibe um gráfico mostrando o tráfego de rede recebido e enviado por todas as interfaces de rede no nó, site ou grade.

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

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

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

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Informações relacionadas

["Monitorar conexões de rede e desempenho"](#)

Exibir a guia armazenamento

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

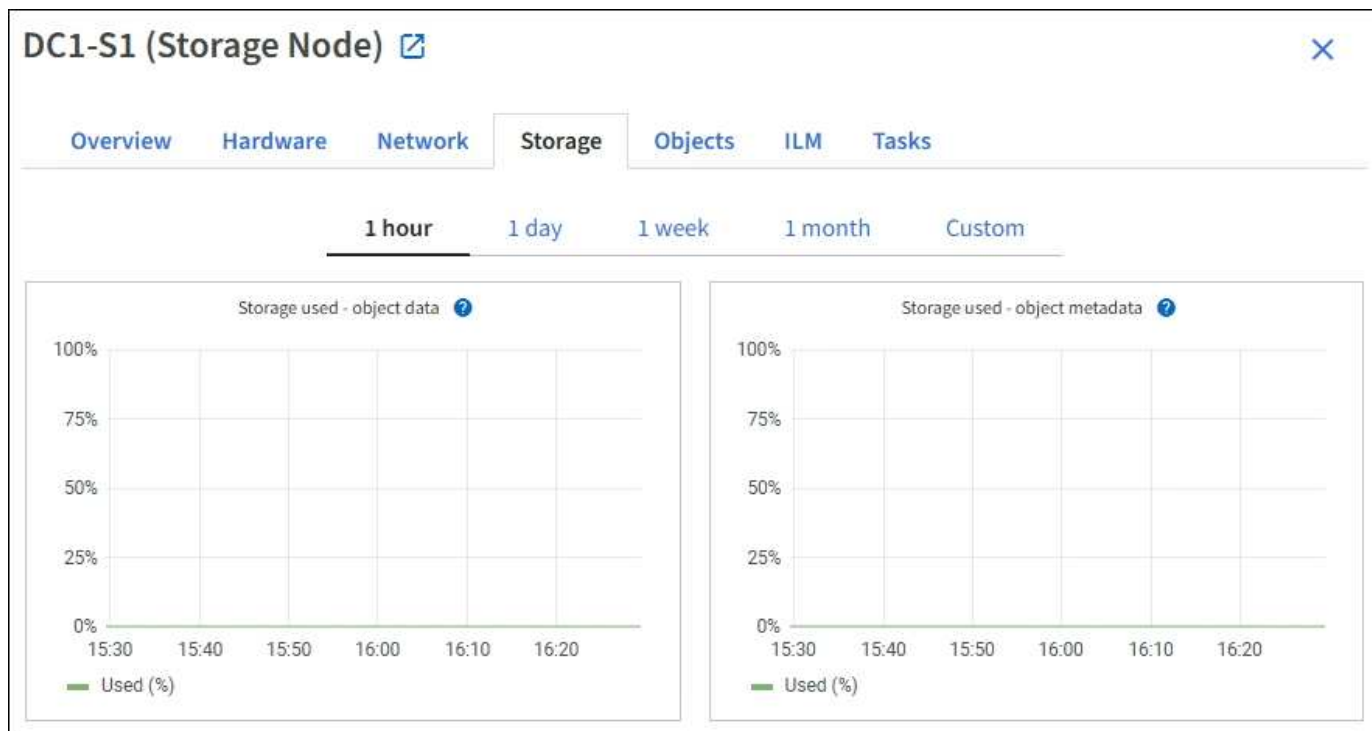
A guia Storage (armazenamento) é exibida para todos os nós, cada local e toda a grade.

Armazenamento de gráficos usados

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



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




Dispositivos de disco, volumes e objetos armazenam tabelas

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










Disk devices

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

Volumes

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

Object stores

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

Informações relacionadas

["Monitorar a capacidade de armazenamento"](#)

Exibir a guia objetos

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

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

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Object counts

Total objects: ? 1,295

Lost objects: ? 0

S3 buckets and Swift containers: ? 161

Metadata store queries

Average latency: ? 10.00 milliseconds

Queries - successful: ? 14,587

Queries - failed (timed out): ? 0

Queries - failed (consistency level unmet): ? 0

Verification

Status: ? No errors

Percent complete: ? 47.14%

Average stat time: ? 0.00 microseconds

Objects verified: ? 0

Object verification rate: ? 0.00 objects / second

Data verified: ? 0 bytes

Data verification rate: ? 0.00 bytes / second

Missing objects: ? 0

Corrupt objects: ? 0

Corrupt objects unidentified: ? 0

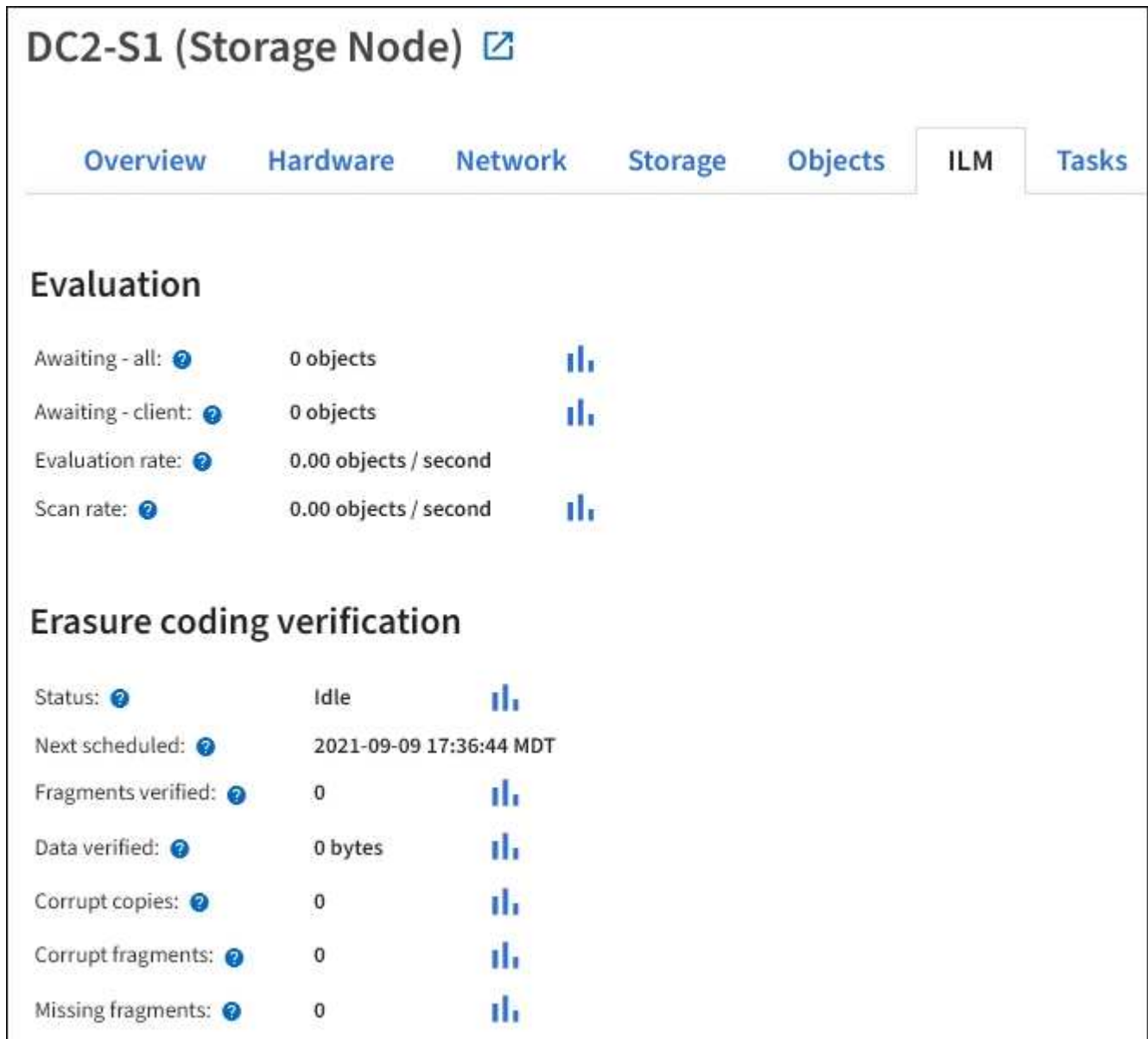
Quarantined objects: ? 0

Veja a guia ILM

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

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

Para nós de storage, a guia ILM fornece detalhes sobre a avaliação ILM e a verificação em segundo plano para objetos codificados por apagamento.



Informações relacionadas

["Monitorar o gerenciamento do ciclo de vida das informações"](#)

["Administrar o StorageGRID"](#)

Use a guia tarefas

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

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

- ["Renomeie grade, sites e nós"](#)
- ["Reinicie o nó da grade"](#)
- ["Coloque o aparelho no modo de manutenção"](#)

Veja a guia balanceador de carga

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

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

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



Solicitar tráfego

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



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

Taxa de solicitação recebida

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

Duração média da solicitação (sem erro)

Este gráfico fornece uma média móvel de 3 minutos de duração de solicitações, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Cada duração da solicitação começa quando um cabeçalho de solicitação é analisado pelo serviço Load Balancer e termina quando o corpo de resposta

completo é retornado ao cliente.

Taxa de resposta de erro

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

Informações relacionadas

["Monitorar operações de balanceamento de carga"](#)

["Administrar o StorageGRID"](#)

Veja a guia Serviços da Plataforma

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

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

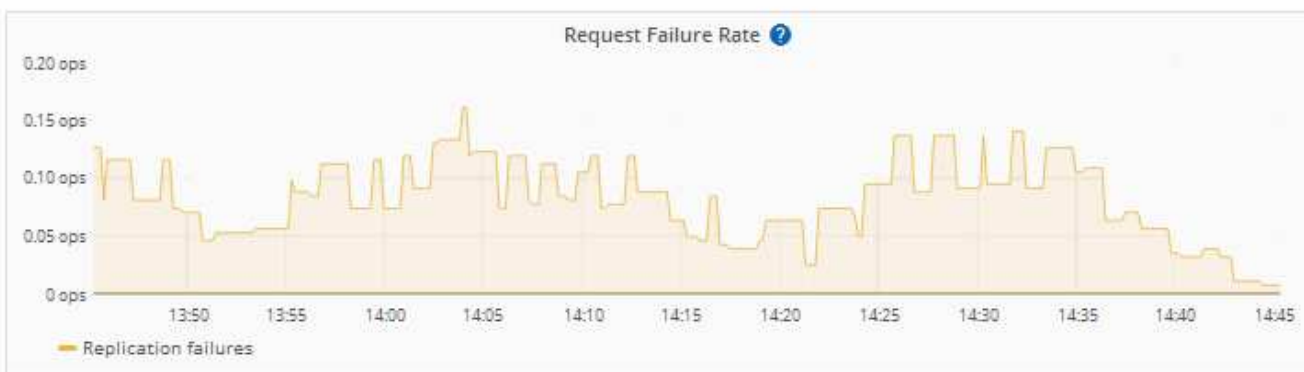
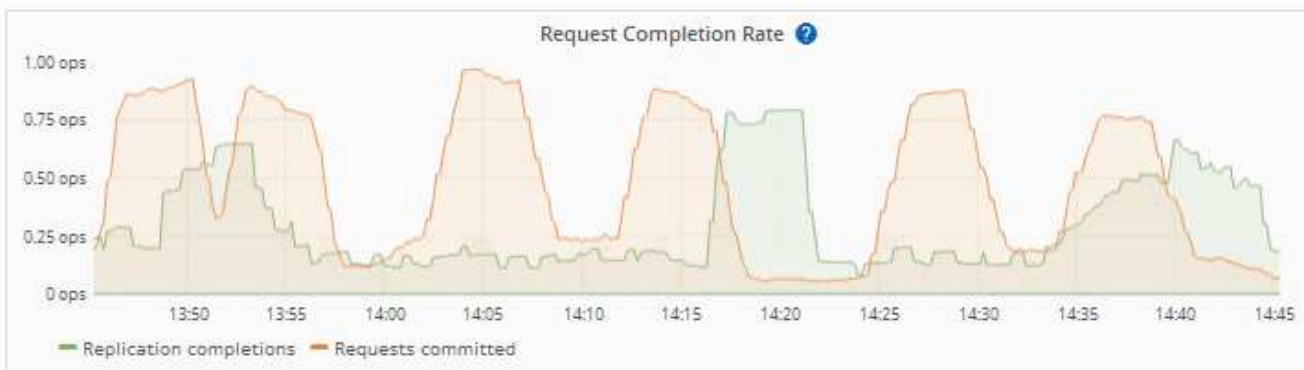
1 hour

1 day

1 week

1 month

Custom



Para obter mais informações sobre os serviços da plataforma S3, incluindo detalhes de solução de problemas, consulte o ["Instruções para administrar o StorageGRID"](#).

Exibir a guia Gerenciar unidades (somente SGF6112)

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



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

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

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

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

Para obter informações sobre como usar a guia Gerenciar unidades, ["Use a guia Gerenciar unidades"](#) consulte .

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

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



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

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

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



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

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



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



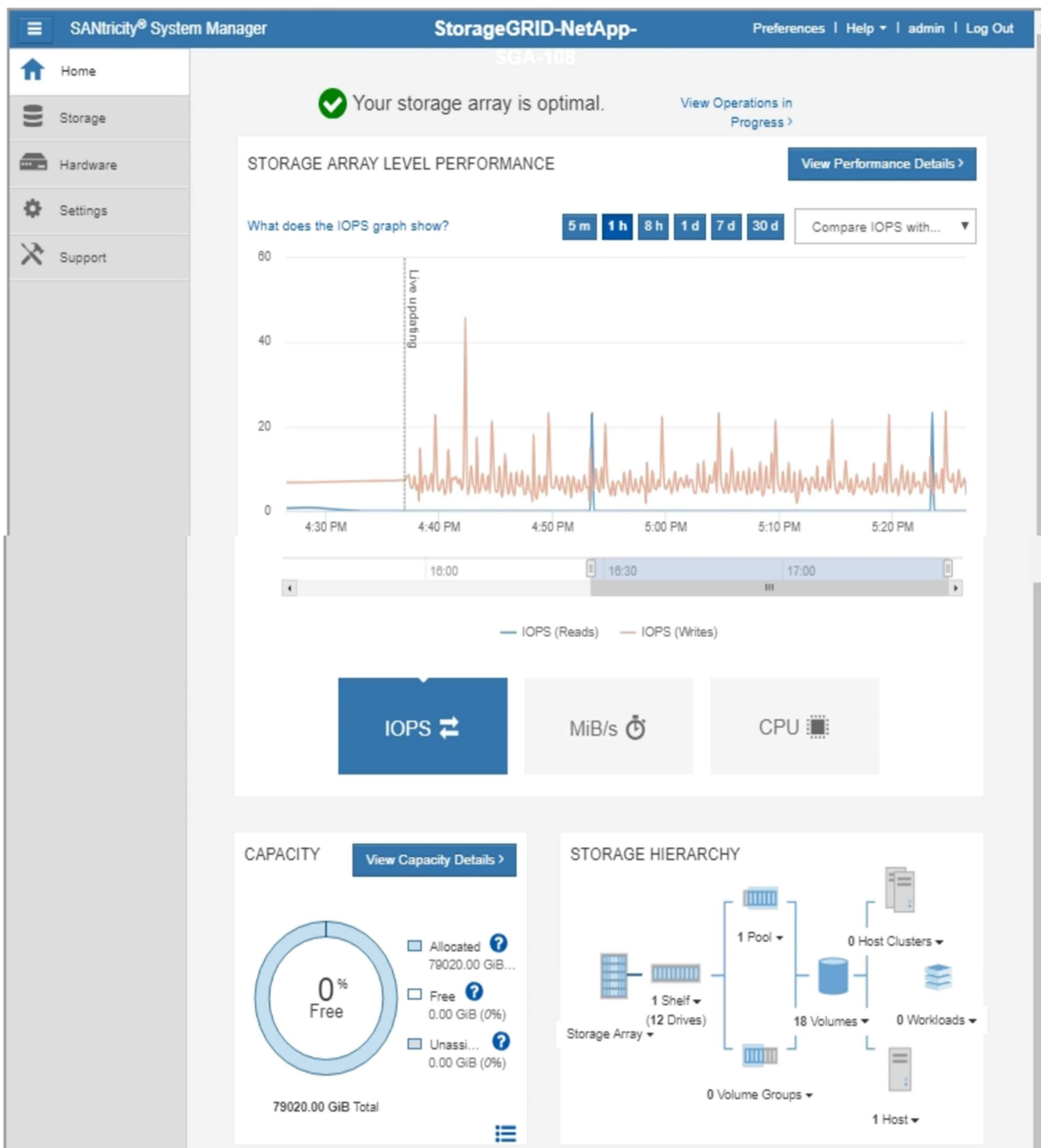
O acesso ao Gerenciador de sistemas do SANtricity a partir do Gerenciador de Grade geralmente se destina apenas a monitorar o hardware do dispositivo e configurar o e-Series AutoSupport. Muitos recursos e operações dentro do Gerenciador de sistema do SANtricity, como atualização de firmware, não se aplicam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

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

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



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

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

cada gráfico.

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

Informações para monitorar regularmente

O que e quando monitorar

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

Antes de começar

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

Sobre tarefas de monitoramento

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

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

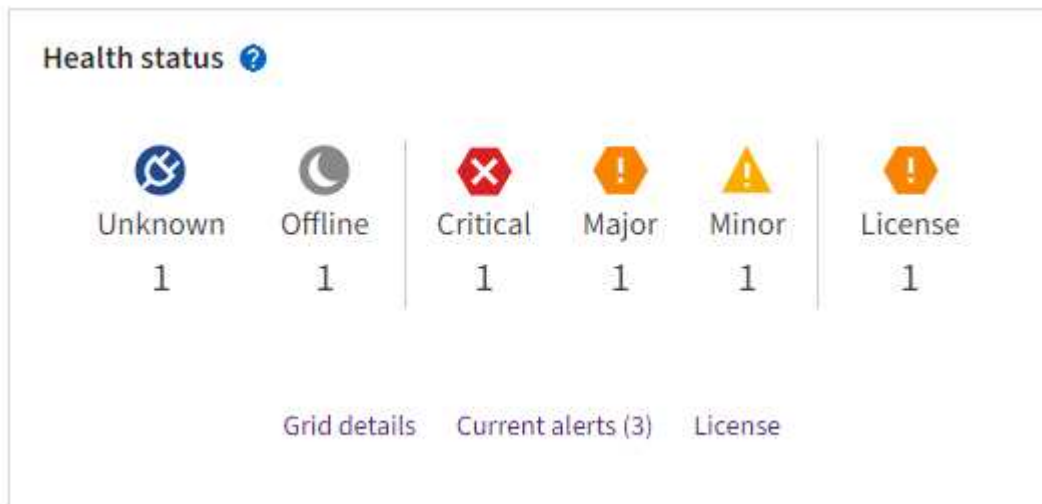
Monitorar a integridade do sistema

Monitore diariamente a integridade geral do seu sistema StorageGRID.

Sobre esta tarefa

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

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






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

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

Monitorar os estados de conexão do nó

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

Ícone	Descrição	Ação necessária
	<p>Não ligado - desconhecido</p> <p>Por um motivo desconhecido, um nó é desconetado ou os serviços no nó estão inalterados inesperadamente. Por exemplo, um serviço no nó pode ser interrompido ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada.</p> <p>O alerta não é possível se comunicar com o nó também pode ser acionado. Outros alertas também podem estar ativos.</p>	<p>Requer atenção imediata. Selecione cada alerta e siga as ações recomendadas.</p> <p>Por exemplo, talvez seja necessário reiniciar um serviço que tenha parado ou reiniciado o host para o nó.</p> <p>Nota: Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.</p>
	<p>Não conectado - administrativamente para baixo</p> <p>Por um motivo esperado, o nó não está conectado à grade.</p> <p>Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.</p> <p>Com base no problema subjacente, esses nós geralmente voltam online sem nenhuma intervenção.</p>	<p>Determine se algum alerta está afetando esse nó.</p> <p>Se um ou mais alertas estiverem ativos selecione cada alerta e siga as ações recomendadas.</p>
	<p>Conectado</p> <p>O nó está conectado à grade.</p>	Nenhuma ação necessária.

Ver alertas atuais e resolvidos

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

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

Opcionalmente, você assistiu ao vídeo: "[Vídeo: Visão geral dos alertas para o StorageGRID 11,8](#)"



A tabela a seguir descreve as informações mostradas no Gerenciador de Grade para alertas atuais e resolvidos.

Cabeçalho da coluna	Descrição
Nome ou título	O nome do alerta e sua descrição.
Gravidade	<p>A gravidade do alerta. Para alertas atuais, se vários alertas forem agrupados, a linha de título mostra quantas instâncias desse alerta estão ocorrendo em cada gravidade.</p> <p> Crítico: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido.</p> <p> Major: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID.</p> <p> Menor: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.</p>
Tempo acionado	<p>Alertas atuais: A data e a hora em que o alerta foi acionado na sua hora local e em UTC. Se vários alertas forem agrupados, a linha de título mostrará horas para a instância mais recente do alerta (<i>newest</i>) e a instância mais antiga do alerta (<i>older</i>).</p> <p>Alertas resolvidos: Há quanto tempo o alerta foi acionado.</p>
Local/nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.
Estado	Se o alerta está ativo, silenciado ou resolvido. Se vários alertas forem agrupados e todos os alertas estiverem selecionados na lista suspensa, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.
Tempo resolvido (apenas alertas resolvidos)	Há quanto tempo o alerta foi resolvido.
Valores atuais ou <i>valores de dados</i>	<p>O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta armazenamento de dados de objeto baixo incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.</p> <p>Nota: se vários alertas atuais forem agrupados, os valores atuais não serão exibidos na linha de título.</p>

Cabeçalho da coluna	Descrição
Valores acionados (apenas alertas resolvidos)	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, são apresentados valores adicionais para o ajudar a compreender e investigar o alerta. Por exemplo, os valores mostrados para um alerta armazenamento de dados de objeto baixo incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

Passos

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

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

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

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

2. Para expandir grupos de alertas, selecione o cursor para baixo ▼. Para recolher alertas individuais num grupo, selecione o cursor para cima ▲ ou selecione o nome do grupo.
3. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **alertas de grupo**.
4. Para classificar os alertas atuais ou grupos de alertas, selecione as setas para cima/para baixo ⬆⬇ em cada cabeçalho de coluna.
 - Quando **alertas de grupo** é selecionado, tanto os grupos de alerta quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **tempo disparado** para encontrar a instância mais recente de um alerta específico.
 - Quando **alertas de grupo** é limpo, toda a lista de alertas é classificada. Por exemplo, você pode querer classificar todos os alertas por **nó/Site** para ver todos os alertas que afetam um nó específico.
5. Para filtrar os alertas atuais por status (**todos os alertas**, **Ativo** ou **silenciado**, use o menu suspenso na parte superior da tabela.

["Silenciar notificações de alerta"](#) Consulte .

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

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

Você deve ter a ["Gerencie alertas ou permissão de acesso root"](#) regra para silenciar uma regra de alerta.



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

9. Para visualizar as condições atuais da regra de alerta:

- a. Nos detalhes do alerta, selecione **Ver condições**.

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

- b. Para fechar o pop-up, clique em qualquer lugar fora do pop-up.

10. Opcionalmente, selecione **Editar regra** para editar a regra de alerta que fez com que esse alerta fosse acionado.

Você deve ter o ["Gerencie alertas ou permissão de acesso root"](#) para editar uma regra de alerta.



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

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

Monitorar a capacidade de armazenamento

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

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

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

Monitore a capacidade de armazenamento de toda a grade

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

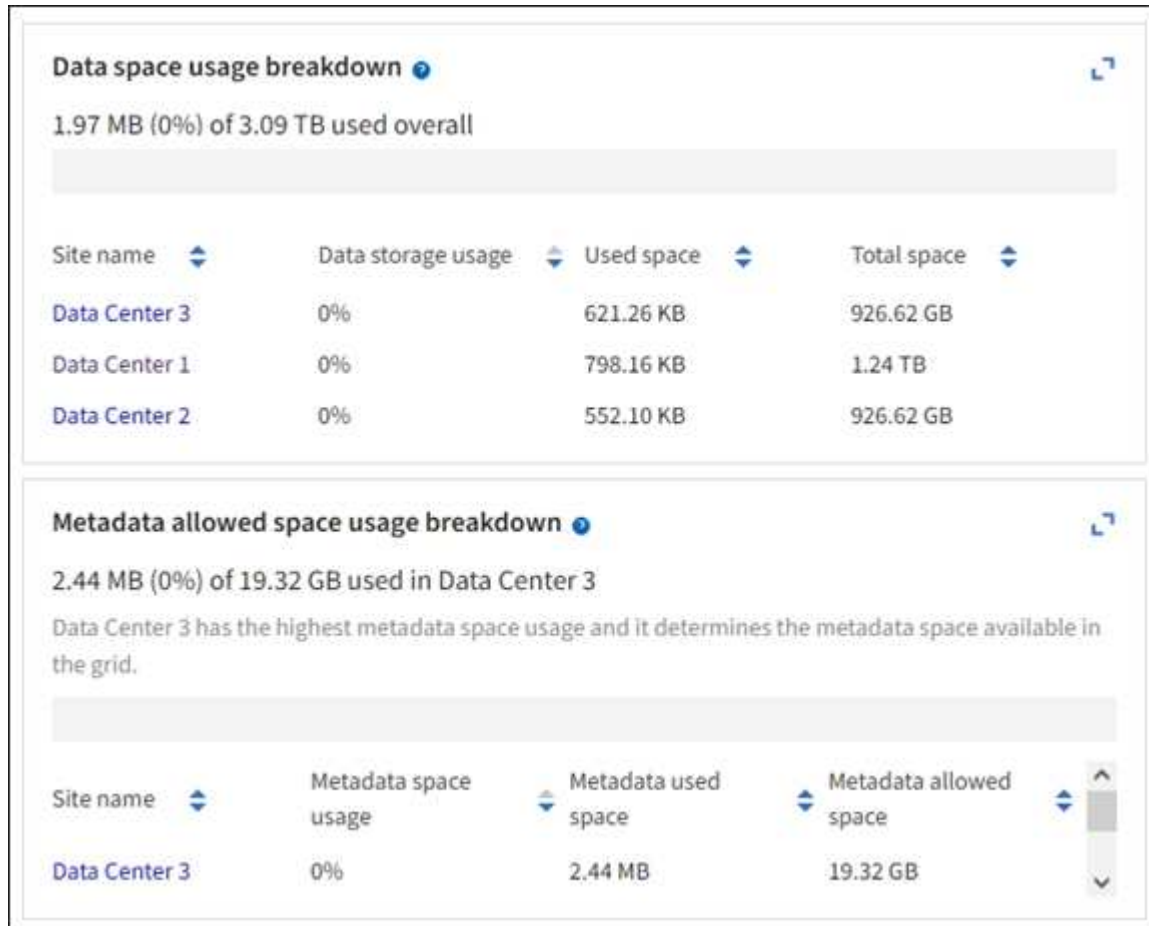
O painel do Grid Manager permite avaliar rapidamente a quantidade de armazenamento disponível para toda a grade e para cada data center. A página nós fornece valores mais detalhados para dados de objetos e metadados de objetos.

Passos

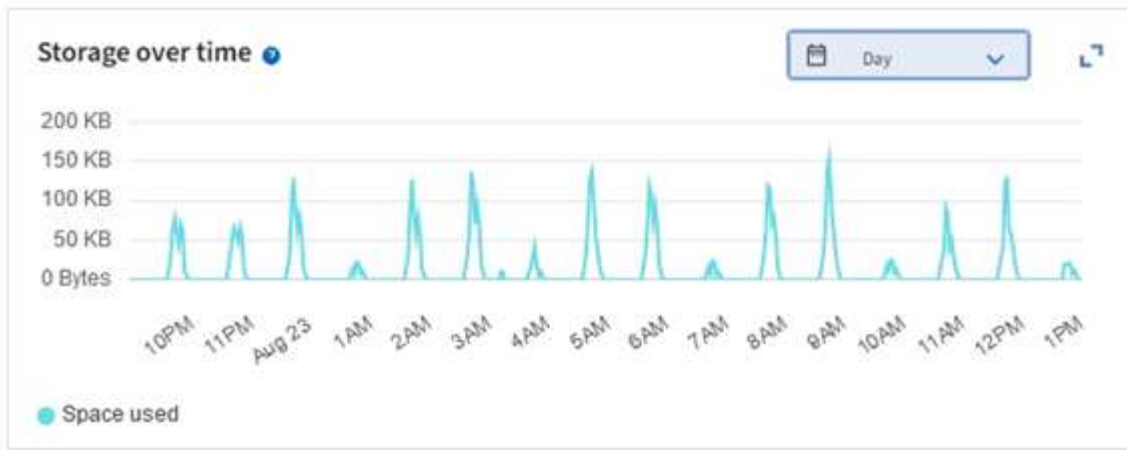
1. Avalie a quantidade de storage disponível para toda a grade e para cada data center.
 - a. Selecione **Painel > Visão geral**.
 - b. Observe os valores na divisão de uso de espaço de dados e nos cartões de divisão de uso de espaço de metadados permitidos. Cada cartão lista uma porcentagem do uso do armazenamento, a capacidade do espaço usado e o espaço total disponível ou permitido pelo local.



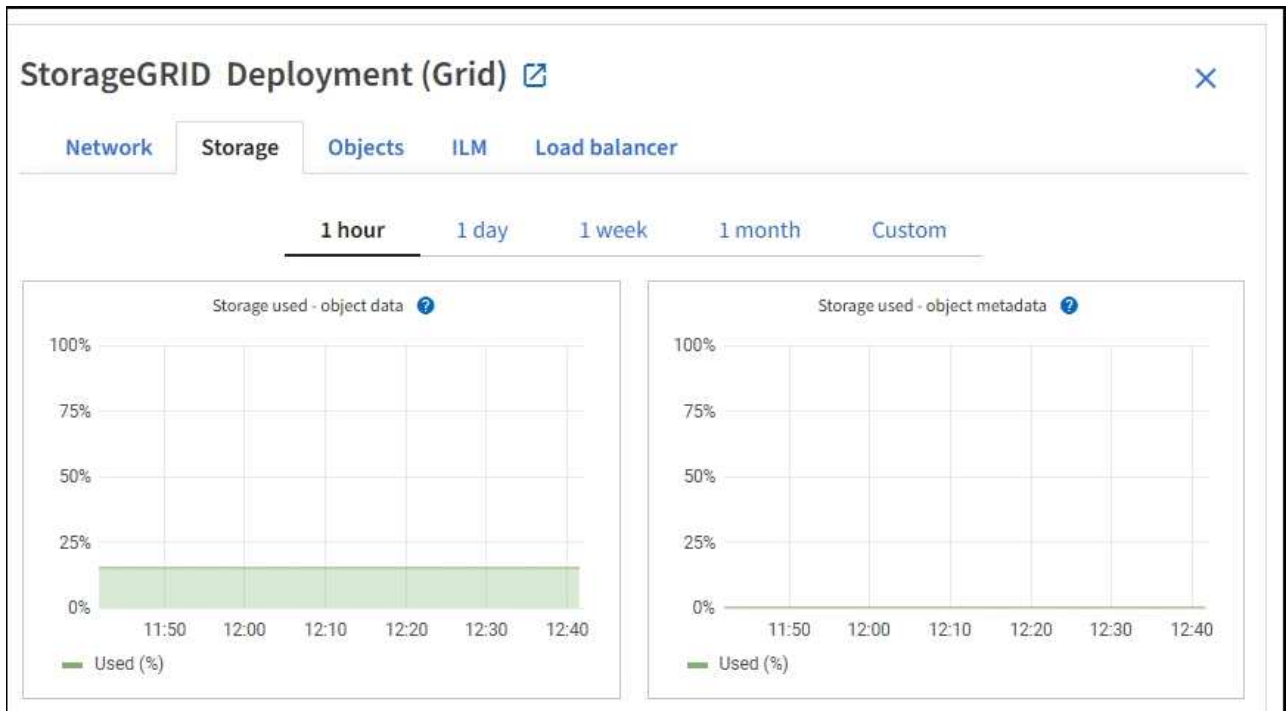
O resumo não inclui Mídia de arquivamento.



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



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



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



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

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

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



Se sua política de ILM usa codificação de apagamento, talvez você prefira expandir quando os nós de storage existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que precisam ser adicionados.

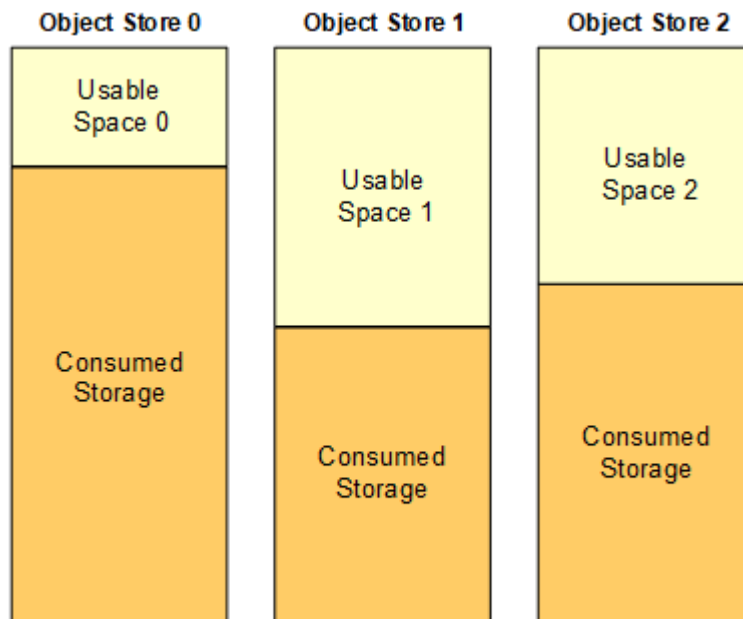
Para obter mais informações sobre como Planejar uma expansão de armazenamento, consulte o ["Instruções para expandir StorageGRID"](#).

Monitore a capacidade de storage para cada nó de storage

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

Sobre esta tarefa

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



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Passos

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

Os gráficos e tabelas para o nó aparecem.

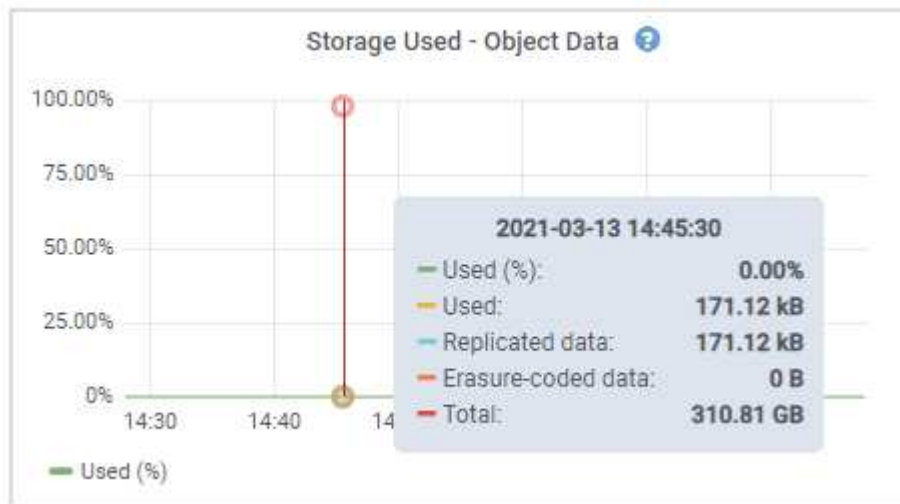
2. Posicione o cursor sobre o gráfico armazenamento usado - dados do objeto.

São apresentados os seguintes valores:

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


por apagamento neste nó, site ou grade.

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



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



Para visualizar gráficos destes valores, clique nos ícones de gráfico  nas colunas disponíveis.

Disk devices

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

Volumes

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

Object stores

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

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

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



Se sua política de ILM usa codificação de apagamento, talvez você prefira expandir quando os nós de storage existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que precisam ser adicionados.

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

"Instruções para expandir StorageGRID".

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

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

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

Sobre esta tarefa

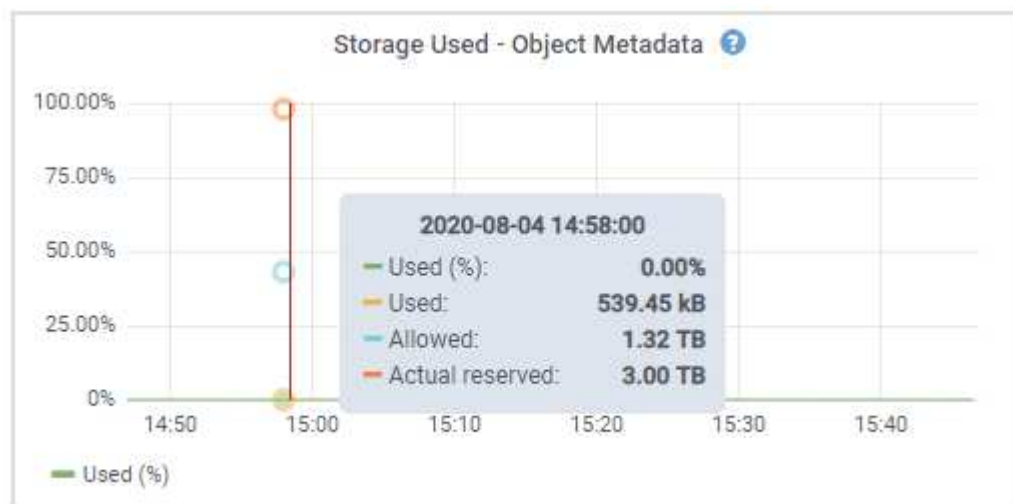
O StorageGRID mantém três cópias de metadados de objetos em cada local para fornecer redundância e proteger os metadados de objetos da perda. As três cópias são distribuídas uniformemente por todos os nós de storage em cada local, usando o espaço reservado para metadados no volume de storage 0 de cada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

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

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

Passos

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



Usado (%)

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

Métricas de Prometheus: `storagegrid_storage_utilization_metadata_bytes` E `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

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

Métrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

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

Métrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Real reservado

O espaço real reservado para metadados neste nó de storage. Inclui o espaço permitido e o espaço necessário para operações essenciais de metadados. Para saber como esse valor é calculado para cada nó de armazenamento, consulte "[Descrição completa do espaço reservado real para metadados](#)".

Prometheus métrica será adicionada em uma versão futura.



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

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



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

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

Monitorar previsões de uso de espaço

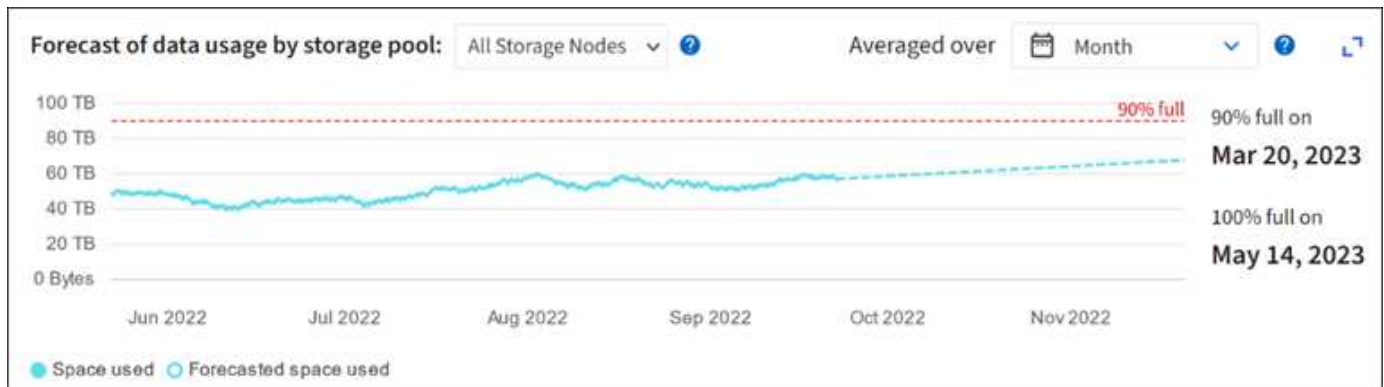
Monitore as previsões de uso de espaço para dados e metadados do usuário para estimar quando será "[expanda uma grade](#)" necessário .

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

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

Passos

- No painel de instrumentos, selecione **armazenamento**.
- Visualize as placas do painel, a previsão do uso de dados por pool de armazenamento e a previsão do uso de metadados por local.
- Use esses valores para estimar quando será necessário adicionar novos nós de storage para storage de dados e metadados.



Monitorar o gerenciamento do ciclo de vida das informações

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

Sobre esta tarefa

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

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

Use a guia Painel do Gerenciador de Grade

Passos

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

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

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

Use a página NÓS

Passos

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



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

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



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

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



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

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



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

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

Monitorar recursos de rede e do sistema

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

Monitorar conexões de rede e desempenho

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

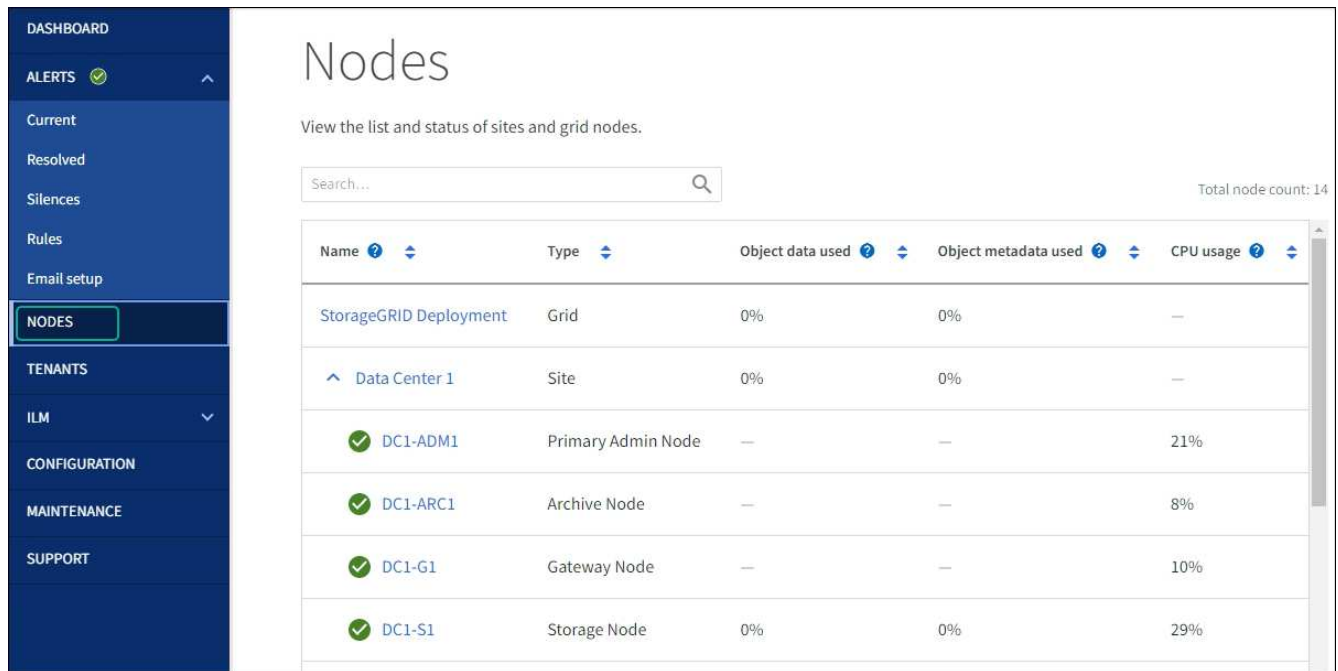
Use o Gerenciador de Grade para monitorar a conectividade e o desempenho da rede, para que você possa resolver quaisquer problemas imediatamente.

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

Passos

1. Selecione **NODES**.

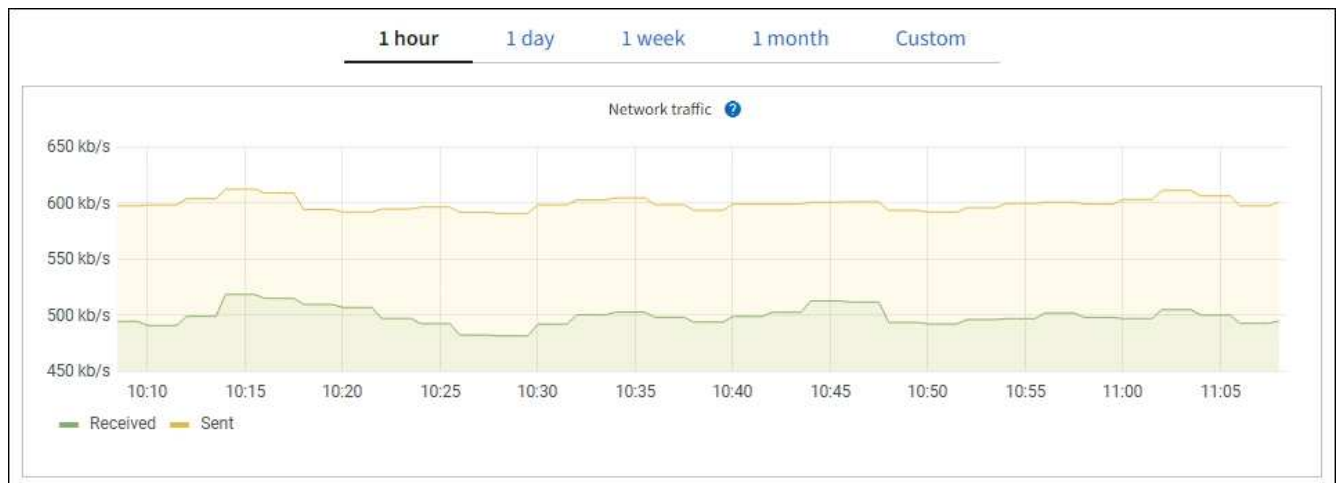
A página nós é exibida. Cada nó na grade é listado no formato de tabela.



Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

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

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



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

página.

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

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

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

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

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

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

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

<div><div>+ Create</div><div>Edit</div><div>Remove</div><div>Metrics</div></div>		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b
Displaying 2 traffic classification policies.		

- a. Para exibir gráficos que mostram as métricas de rede associadas a uma política, selecione o botão de opção à esquerda da política e clique em **métricas**.
- b. Reveja os gráficos para compreender o tráfego de rede associado à política.

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

frequência com que o tráfego é limitado e decida se a política continua atendendo às suas necessidades. De tempos em tempos [ajuste cada política de classificação de tráfego conforme necessário](#), .

Informações relacionadas

["Veja a guia rede"](#)

["Monitorar os estados de conexão do nó"](#)

Monitore os recursos no nível do nó

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

Passos

1. Na página **NÓS**, selecione o nó.
2. Selecione a guia **hardware** para exibir gráficos de utilização da CPU e uso da memória.



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

Informações relacionadas

["Exibir informações sobre os nós de storage do dispositivo"](#)

["Exibir informações sobre os nós de administração do dispositivo e os nós de gateway"](#)

Monitorar a atividade do locatário

Todas as atividades dos clientes S3 e Swift estão associadas às contas de inquilino do StorageGRID. Você pode usar o Gerenciador de Grade para monitorar o uso do armazenamento ou o tráfego de rede para todos os locatários ou um locatário específico. Você pode usar o log de auditoria ou os painéis do Grafana para reunir informações mais detalhadas sobre como os locatários estão usando o StorageGRID.

Antes de começar

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

Ver todos os inquilinos

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

Passos

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

O espaço lógico usado, a utilização da cota, a cota e a contagem de objetos são listados para cada locatário. Se uma cota não for definida para um locatário, os campos utilização da cota e quota contêm um traço (& n.o 8212;).



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

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions	<input type="text" value="Search tenants by name or ID"/>		Displaying 5 results		
<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL	
<input type="checkbox"/>	Tenant 01	2.00 GB	<div><div></div></div> 10%	20.00 GB	100	→	📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div><div></div></div> 85%	100.00 GB	500	→	📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div><div></div></div> 50%	1.00 PB	10,000	→	📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div><div></div></div> 95%	500.00 TB	50,000	→	📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→	📄

3. Opcionalmente, faça login em uma conta de locatário selecionando o link de login [→](#) na coluna **Sign in/Copy URL**.
4. Opcionalmente, copie o URL da página de login de um locatário selecionando o link URL de cópia [📄](#) na coluna **entrar/Copiar URL**.

5. Opcionalmente, selecione **Exportar para CSV** para exibir e exportar um .csv arquivo contendo os valores de uso para todos os locatários.

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

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

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

Você pode abrir o .csv arquivo em um aplicativo de Planilha ou usá-lo em automação.

6. Se nenhum objeto estiver listado, opcionalmente, selecione **ações > Excluir** para remover um ou mais inquilinos. ["Eliminar conta de inquilino"](#)Consulte .

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

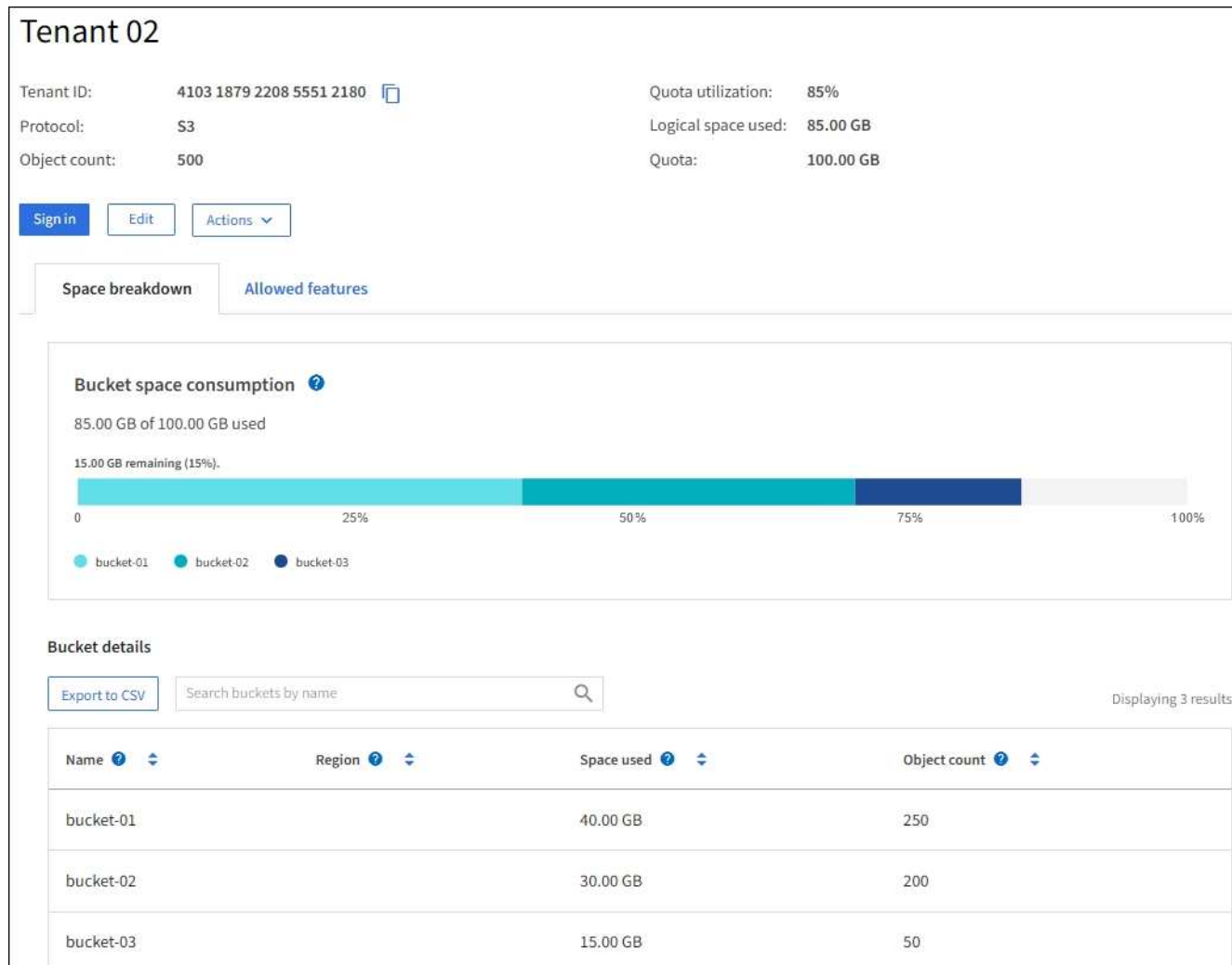
Exibir um locatário específico

Você pode exibir detalhes de um locatário específico.

Passos

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

A página de detalhes do locatário é exibida.



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

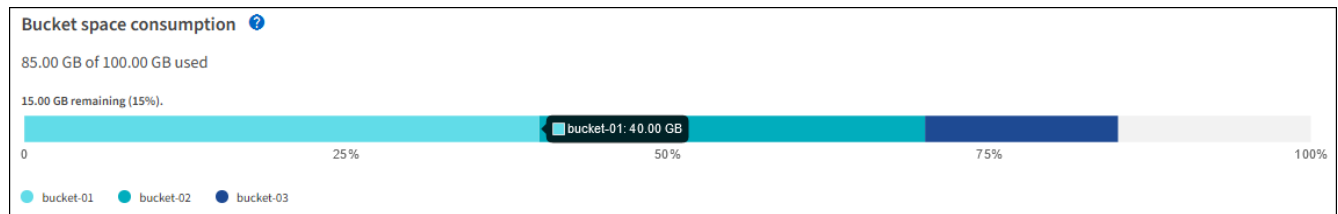
Esta seção da página de detalhes fornece informações resumidas para o locatário, incluindo a contagem de objetos do locatário, a utilização da cota, o espaço lógico usado e a configuração da cota.

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

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

Se uma cota foi definida para esse locatário, a quantidade de cota usada e restante será exibida no texto (por exemplo, 85.00 GB of 100 GB used). Se nenhuma cota foi definida, o locatário tem uma cota ilimitada e o texto inclui apenas uma quantidade de espaço usada (por exemplo, 85.00 GB used). O gráfico de barras mostra a porcentagem de cota em cada bucket ou contentor. Se o inquilino tiver excedido a cota de armazenamento em mais de 1% e em pelo menos 1 GB, o gráfico mostrará a cota total e a quantidade excedente.

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



A utilização de quotas baseia-se em estimativas internas e pode ser ultrapassada em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novos ingere se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em conta o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que a utilização da cota seja recalculada. Os cálculos de utilização de cotas podem levar 10 minutos ou mais.



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



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

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

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

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

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

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

Você pode abrir o .csv arquivo em um aplicativo de Planilha ou usá-lo em automação.

6. Opcionalmente, selecione a guia **recursos permitidos** para ver uma lista das permissões e recursos que estão habilitados para o locatário. "[Editar conta de locatário](#)"Veja se você precisa alterar qualquer uma dessas configurações.

7. Se o locatário tiver a permissão **usar conexão de federação de grade**, selecione opcionalmente a guia **federação de grade** para saber mais sobre a conexão.

"O que é a federação de grade?"Consulte e "[Gerenciar os locatários permitidos para a federação de grade](#)".

Ver o tráfego de rede

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

Passos

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

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

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

Consulte "[Gerenciar políticas de classificação de tráfego](#)" para obter mais informações.

Use o log de auditoria

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

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

- Operações específicas do cliente, como COLOCAR, OBTER ou EXCLUIR
- Tamanhos de objetos
- A regra ILM aplicada a objetos
- O IP de origem das solicitações do cliente

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

Consulte "[Rever registros de auditoria](#)" para obter mais informações.

Use métricas Prometheus

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

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



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

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

Consulte "[Analise as métricas de suporte](#)" para obter mais informações.

Monitore as operações dos clientes S3 e Swift

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

Antes de começar

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

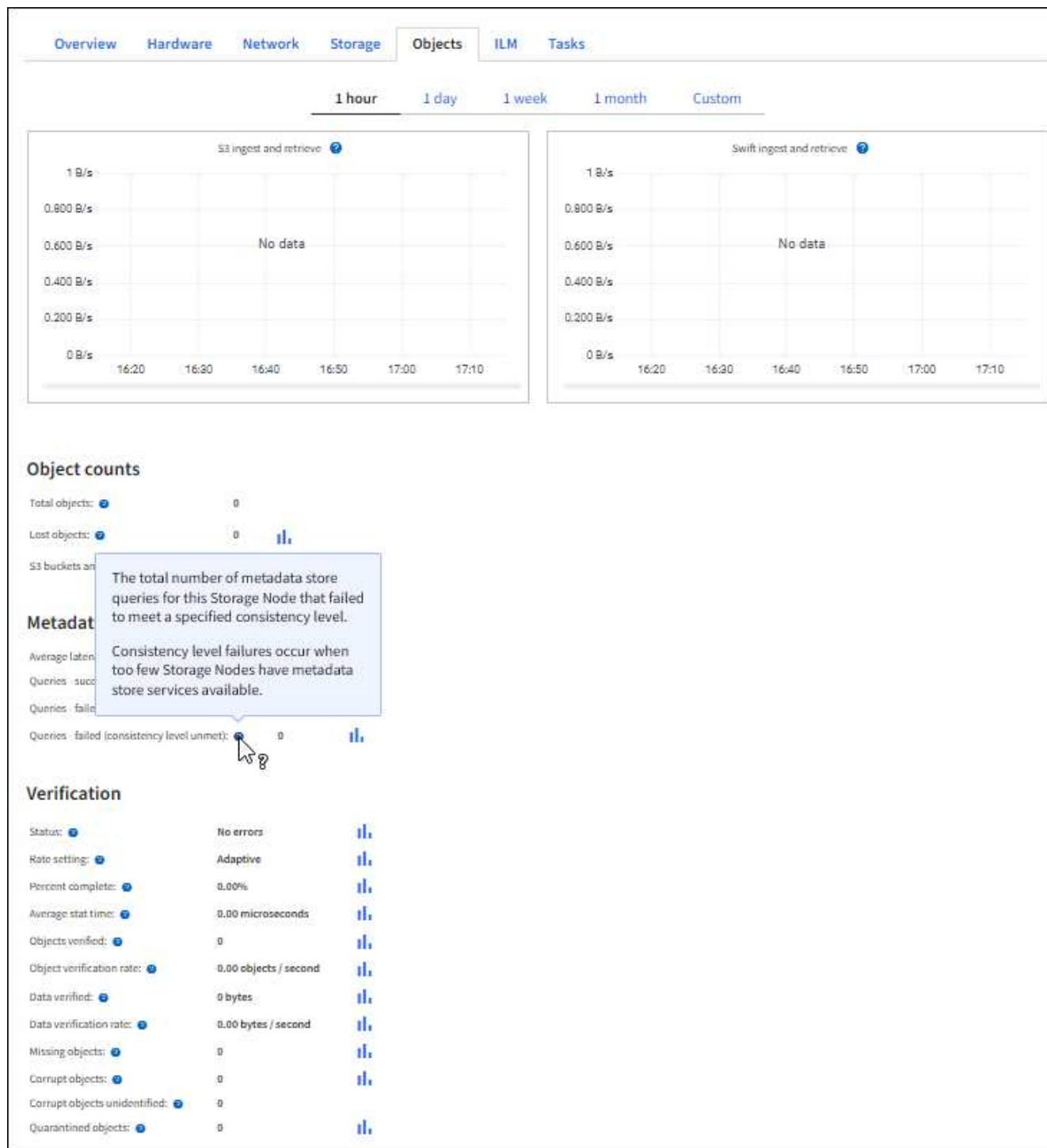
Passos

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

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

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

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



Monitorar operações de balanceamento de carga

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

Sobre esta tarefa

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

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

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

Para obter mais informações, "[Configurar conexões de cliente S3 e Swift](#)" consulte .

Passos

1. Se os clientes S3 ou Swift se conectarem usando o serviço Load Balancer, verifique se os nós Admin ou os nós de Gateway estão distribuindo ativamente o tráfego como você espera:

- a. Selecione **NODES**.
- b. Selecione um nó de gateway ou nó de administrador.
- c. Na guia **Visão geral**, verifique se uma interface de nó está em um grupo de HA e se a interface de nó tem a função de primária.

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

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

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

- f. Revise o gráfico da taxa de solicitação de entrada do Load Balancer da última semana para analisar a taxa de transferência de objetos do nó.
- g. Repita estas etapas para cada nó de administrador ou nó de gateway no sistema StorageGRID.
- h. Opcionalmente, use políticas de classificação de tráfego para visualizar uma análise mais detalhada do tráfego que está sendo servido pelo serviço Load Balancer.

2. Verifique se essas solicitações estão sendo distribuídas uniformemente para os nós de storage.

- a. Selecione **Storage Node > LDR > HTTP**.
- b. Reveja o número de **sessões de entrada atualmente estabelecidas**.
- c. Repita para cada nó de armazenamento na grade.

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

Monitorar conexões de federação de grade

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

Antes de começar

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

Ver todas as ligações

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

Passos

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

A página de federação de grade é exibida.

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

Nesta guia, você pode:

- ["Crie uma nova conexão"](#).
- Selecione uma conexão existente com ["editar ou testar"](#)o .

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

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

Nesta guia, você pode:

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

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

[Connections](#)
[Permitted tenants](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
Tenant A	Grid 1 - Grid 2	Connected	10.96.130.76	Check for errors

Veja uma conexão específica

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

Passos

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

Na página de detalhes da conexão, você pode:

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

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

Nesta guia, você pode:

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

Grid 1 - Grid 2

Local hostname (this grid):

10.96.130.64

Port:

23000

Remote hostname (other grid):

10.96.130.76

Connection status:

✓

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
<div><div></div>Tenant A</div>	<div>Check for errors</div>

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

Nesta guia, você pode:

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

Grid A

Grid B

Local hostname (this grid):
Port:

Remote hostname (other grid):

Connection status:

10.96.106.230
23000
10.96.104.230

Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Rotate certificates

ServerClient

Download certificateCopy certificate PEM

Metadata ?

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230Serial number: 30:81:B8:DD:AE:B2:86:0AIssuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPTIssued on: 2022-10-04T02:21:18.000ZExpires on: 2024-10-03T19:05:13.000ZSHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DFSHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60Alternative names: IP Address:10.96.106.230

Certificate PEM ?

-----BEGIN CERTIFICATE-----MIIGdTCCBF2gAwIBAgIIHIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UEBhhMCVVwMEIxEjARBgNVBAglMCKNhbgGmb3JuaWExeXljAQBGnVBAc/MCVNbmS5dmFsZTEUABTCFAhSCouKvVqOQAAAAAZBANVBAsMFkFLDEFCBZAAGQuNmIdIRlJJ-----

Analise as métricas de replicação entre grades

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

Passos

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



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

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

Para obter instruções detalhadas, "[Análise as métricas de suporte](#)" consulte .

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

Monitorar a capacidade de arquivamento

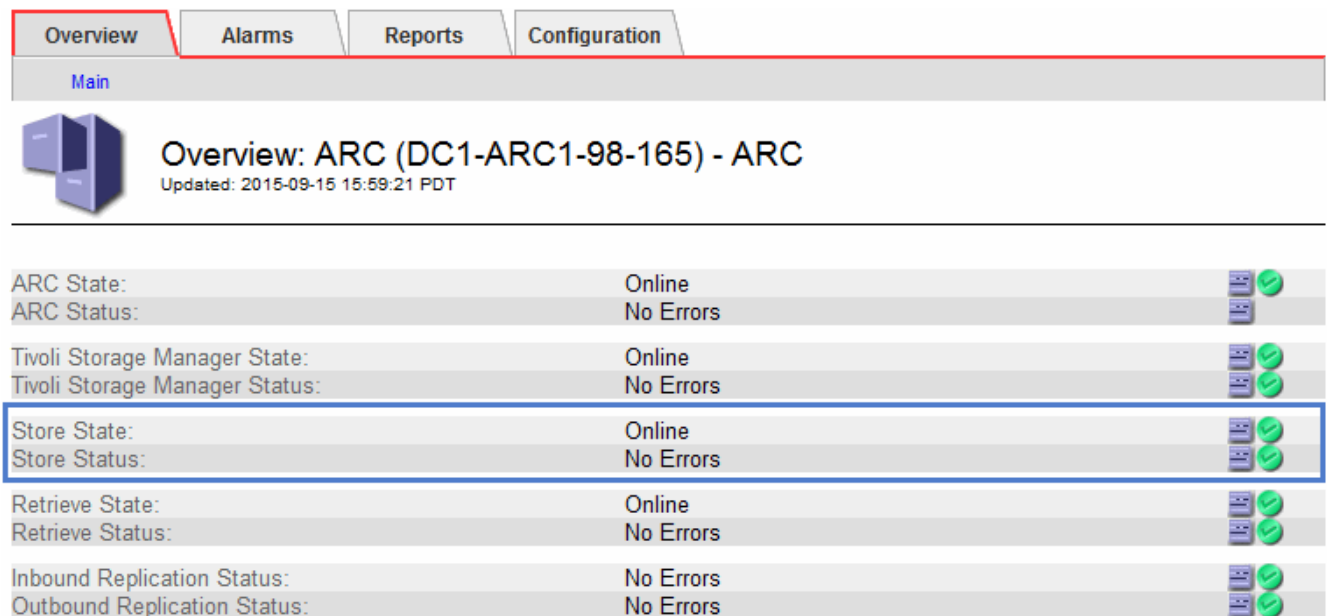
Não é possível monitorar diretamente a capacidade de um sistema de armazenamento de arquivamento externo por meio do sistema StorageGRID. No entanto, você pode monitorar se o nó Arquivo ainda pode enviar dados de objeto para o destino do arquivamento, o que pode indicar que uma expansão de Mídia de arquivamento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






















Sobre esta tarefa

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

Passos

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



Overview	Alarms	Reports	Configuration
Main			
 Overview: ARC (DC1-ARC1-98-165) - ARC Updated: 2015-09-15 15:59:21 PDT			
ARC State:	Online		
ARC Status:	No Errors		
Tivoli Storage Manager State:	Online		
Tivoli Storage Manager Status:	No Errors		
Store State:	Online		
Store Status:	No Errors		
Retrieve State:	Online		
Retrieve Status:	No Errors		
Inbound Replication Status:	No Errors		
Outbound Replication Status:	No Errors		

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

Alertas e alarmes

Gerenciar alertas e alarmes: Visão geral

O sistema de alerta StorageGRID foi concebido para o informar sobre problemas operacionais que requerem a sua atenção. O sistema de alarme legado está obsoleto.

Sistema de alerta

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

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

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

Sistema de alarme legado

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



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

Quando um alarme é acionado, ocorrem as seguintes ações:

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

Compare alertas e alarmes

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

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

	Alertas	Alarmes (sistema legado)
Como posso ver quais alertas ou alarmes estão ativos?	<ul style="list-style-type: none"> • Selecione o link Current alerts no painel. • Selecione o alerta na página NODES > Overview. • Selecione ALERTAS > atual. <p>"Ver alertas atuais"</p>	<p>Selecione SUPPORT > Alarmes (legacy) > Current Alarms.</p> <p>"Gerenciar alarmes (sistema legado)"</p>
O que faz com que um alerta ou um alarme seja acionado?	<p>Os alertas são acionados quando uma expressão Prometheus em uma regra de alerta é avaliada como verdadeira para a condição e duração específicas do gatilho.</p> <p>"Ver regras de alerta"</p>	<p>Os alarmes são acionados quando um atributo StorageGRID atinge um valor limite.</p> <p>"Gerenciar alarmes (sistema legado)"</p>
Se um alerta ou alarme for acionado, como resolvo o problema subjacente?	<p>As ações recomendadas para um alerta estão incluídas nas notificações por e-mail e estão disponíveis nas páginas Alertas no Gerenciador de Grade.</p> <p>Conforme necessário, informações adicionais são fornecidas na documentação do StorageGRID.</p> <p>"Referência de alertas"</p>	<p>Você pode aprender sobre um alarme selecionando o nome do atributo ou pode procurar um código de alarme na documentação do StorageGRID.</p> <p>"Referência de alarmes (sistema legado)"</p>
Onde posso ver uma lista de alertas ou alarmes que foram resolvidos?	<p>Selecione ALERTAS > resolvido.</p> <p>"Ver alertas atuais e resolvidos"</p>	<p>Selecione SUPPORT > Alarmes (legacy) > Alarmes históricos.</p> <p>"Gerenciar alarmes (sistema legado)"</p>
Onde posso gerir as definições?	<p>Selecione ALERTAS > regras.</p> <p>"Gerenciar alertas"</p>	<p>Selecione SUPPORT. Em seguida, use as opções na seção Alarmes (legacy) do menu.</p> <p>"Gerenciar alarmes (sistema legado)"</p>

	Alertas	Alarmes (sistema legado)
Quais permissões do grupo de usuários eu preciso?	<ul style="list-style-type: none"> Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alertas atuais e resolvidos. Você deve ter a permissão Gerenciar alertas para gerenciar silêncios, notificações de alerta e regras de alerta. <p>"Administrar o StorageGRID"</p>	<ul style="list-style-type: none"> Qualquer pessoa que possa entrar no Gerenciador de Grade pode exibir alarmes legados. Você deve ter a permissão de reconhecer alarmes para reconhecer alarmes. Você deve ter a configuração da página de topologia de Grade e outras permissões de configuração de grade para gerenciar alarmes globais e notificações de e-mail. <p>"Administrar o StorageGRID"</p>
Como faço para gerenciar notificações por e-mail?	<p>Selecione ALERTAS > Configuração do e-mail.</p> <p>Nota: como os alarmes e alertas são sistemas independentes, a configuração de e-mail usada para notificações de alarme e AutoSupport não é usada para notificações de alerta. No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações.</p> <p>"Configurar notificações por e-mail para alertas"</p>	<p>Selecione SUPPORT > Alarmes (legacy) > Configuração de e-mail legado.</p> <p>"Gerenciar alarmes (sistema legado)"</p>
Como faço para gerenciar notificações SNMP?	<p>Selecione CONFIGURATION > Monitoring > SNMP Agent.</p> <p>"Utilize a monitorização SNMP"</p>	<i>Não suportado</i>
Como posso controlar quem recebe notificações?	<ol style="list-style-type: none"> Selecione ALERTAS > Configuração do e-mail. Na seção destinatários, insira um endereço de e-mail para cada lista de e-mail ou pessoa que deve receber um e-mail quando ocorrer um alerta. <p>"Configurar notificações por e-mail para alertas"</p>	<ol style="list-style-type: none"> Selecione SUPPORT > Alarmes (legacy) > Configuração de e-mail legado. Criando uma lista de discussão. Selecione notificações. Selecione a lista de discussão. <p>"Gerenciar alarmes (sistema legado)"</p>

	Alertas	Alarmes (sistema legado)
Quais nós de administrador enviam notificações?	Um único nó de administração (o remetente preferido). "O que é um nó de administração?"	Um único nó de administração (o remetente preferido). "O que é um nó de administração?"
Como faço para suprimir algumas notificações?	<ol style="list-style-type: none"> 1. Selecione ALERTAS > silêncios. 2. Selecione a regra de alerta que deseja silenciar. 3. Especifique uma duração para o silêncio. 4. Selecione a gravidade do alerta que deseja silenciar. 5. Selecione para aplicar o silêncio a toda a grade, a um único local ou a um único nó. <p>Nota: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam.</p> <p>"Silenciar notificações de alerta"</p>	<ol style="list-style-type: none"> 1. Selecione SUPPORT > Alarmes (legacy) > Configuração de e-mail legado. 2. Selecione notificações. 3. Selecione uma lista de discussão e selecione suprimir. <p>"Gerenciar alarmes (sistema legado)"</p>
Como faço para suprimir todas as notificações?	<p>Selecione ALERTAS > silêncios.em seguida, selecione todas as regras.</p> <p>Nota: Se você ativou o agente SNMP, os silêncios também suprimem traps SNMP e informam.</p> <p>"Silenciar notificações de alerta"</p>	<i>Não suportado</i>
Como posso personalizar as condições e os gatilhos?	<ol style="list-style-type: none"> 1. Selecione ALERTAS > regras. 2. Selecione uma regra padrão para editar ou selecione criar regra personalizada. <p>"Editar regras de alerta"</p> <p>"Crie regras de alerta personalizadas"</p>	<ol style="list-style-type: none"> 1. Selecione SUPPORT > Alarmes (legacy) > Alarmes globais. 2. Crie um alarme personalizado global para substituir um alarme padrão ou para monitorar um atributo que não tenha um alarme padrão. <p>"Gerenciar alarmes (sistema legado)"</p>

	Alertas	Alarmes (sistema legado)
Como posso desativar um alerta individual ou um alarme?	<ol style="list-style-type: none"> 1. Selecione ALERTAS > regras. 2. Selecione a regra e selecione Editar regra. 3. Desmarque a caixa de seleção Enabled. <p>"Desativar regras de alerta"</p>	<ol style="list-style-type: none"> 1. Selecione SUPPORT > Alarmes (legacy) > Alarmes globais. 2. Selecione a regra e selecione o ícone Editar. 3. Desmarque a caixa de seleção Enabled. <p>"Gerenciar alarmes (sistema legado)"</p>



Gerenciar alertas

Gerenciar alertas: Visão geral

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

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

Para saber mais:


- Reveja o vídeo: ["Vídeo: Visão geral dos alertas para o StorageGRID 11,8"](#)

- Reveja o vídeo: ["Vídeo: Usando métricas para criar alertas personalizados no StorageGRID 11,8"](#)

- Consulte ["Referência de alertas"](#).

Ver regras de alerta

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

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

Antes de começar

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


Passos

1. Selecione **ALERTAS > regras**.

A página regras de alerta é exibida.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.




You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

<div><div>+ Create custom rule</div><div><div>Edit rule</div><div>Remove custom rule</div></div></div>			
Name	Conditions	Type	Status
<div><div></div><div>Appliance battery expired</div><div>The battery in the appliance's storage controller has expired.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance battery failed</div><div>The battery in the appliance's storage controller has failed.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance battery has insufficient learned capacity</div><div>The battery in the appliance's storage controller has insufficient learned capacity.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_BATTERY_WARN")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance battery near expiration</div><div>The battery in the appliance's storage controller is nearing expiration.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance battery removed</div><div>The battery in the appliance's storage controller is missing.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance battery too hot</div><div>The battery in the appliance's storage controller is overheated.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance cache backup device failed</div><div>A persistent cache backup device has failed.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance cache backup device insufficient capacity</div><div>There is insufficient cache backup device capacity.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance cache backup device write-protected</div><div>A cache backup device is write-protected.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED")</div> <div>Major > 0</div>	Default	Enabled
<div><div></div><div>Appliance cache memory size mismatch</div><div>The two controllers in the appliance have different cache sizes.</div></div>	<div>storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH")</div> <div>Major > 0</div>	Default	Enabled

Displaying 62 alert rules.

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

Cabeçalho da coluna	Descrição
Nome	O nome exclusivo e a descrição da regra de alerta. As regras de alerta personalizadas são listadas primeiro, seguidas pelas regras de alerta padrão. O nome da regra de alerta é o assunto das notificações por e-mail.

Cabeçalho da coluna	Descrição
Condições	<p>As expressões Prometheus que determinam quando esse alerta é acionado. Um alerta pode ser acionado em um ou mais dos seguintes níveis de gravidade, mas não é necessária uma condição para cada gravidade.</p> <ul style="list-style-type: none"> • Crítico : existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido. • Major : existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID. • Minor : o sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se ele continuar. Você deve monitorar e resolver alertas menores que não sejam claros por conta própria para garantir que eles não resultem em um problema mais sério.
Tipo	<p>O tipo de regra de alerta:</p> <ul style="list-style-type: none"> • Default: Uma regra de alerta fornecida com o sistema. Você pode desativar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Não é possível remover uma regra de alerta padrão. • Padrão*: Uma regra de alerta padrão que inclui uma condição ou duração editada. Conforme necessário, você pode reverter facilmente uma condição modificada de volta ao padrão original. • Custom: Uma regra de alerta que você criou. Você pode desativar, editar e remover regras de alerta personalizadas.
Estado	<p>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.</p>

Crie regras de alerta personalizadas

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).
- Você está familiarizado com o ["Métricas de Prometheus comumente usadas"](#).

- Você entende o "[Sintaxe das consultas Prometheus](#)".
- Opcionalmente, você assistiu o vídeo: "[Vídeo: Usando métricas para criar alertas personalizados no StorageGRID 11,8](#)".



Sobre esta tarefa

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

- Observe as condições para as regras de alerta padrão e use-as como exemplos para suas regras de alerta personalizadas.
- Se você definir mais de uma condição para uma regra de alerta, use a mesma expressão para todas as condições. Em seguida, altere o valor limite para cada condição.
- Verifique cuidadosamente cada condição para erros de digitação e lógica.
- Use apenas as métricas listadas na API de Gerenciamento de Grade.
- Ao testar uma expressão usando a API Grid Management, esteja ciente de que uma resposta "bem-sucedida" pode ser um corpo de resposta vazio (nenhum alerta acionado). Para ver se o alerta é realmente acionado, você pode definir temporariamente um limite para um valor que você espera ser verdadeiro atualmente.

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

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

Passos

1. Selecione **ALERTAS > regras**.

A página regras de alerta é exibida.

2. Selecione **criar regra personalizada**.

A caixa de diálogo criar regra personalizada é exibida.

Create Custom Rule

Enabled ☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

minutes

Cancel

Save

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

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

4. Introduza as seguintes informações:

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

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

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


Uma expressão básica é geralmente da forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

Para ver as métricas disponíveis e testar expressões Prometheus, selecione o ícone de ajuda  e siga o link para a seção métricas da API de Gerenciamento de Grade.

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

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

O padrão é 5 minutos.

- Selecione **Guardar**.

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

Editar regras de alerta

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Sobre esta tarefa

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



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

Passos

1. Selecione **ALERTAS > regras**.

A página regras de alerta é exibida.

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

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

Edit Rule - Low installed node memory

Enabled ☒

Unique Name

Low installed node memory

Description

The amount of installed memory on a node is low.

Recommended Actions (optional)

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Conditions ?

Minor

Major

node_memory_MemTotal_bytes < 24000000000

Critical

node_memory_MemTotal_bytes <= 12000000000

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

2

minutes

Cancel

Save

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

79

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



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



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

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



Não é possível editar essas informações para regras de alerta padrão.

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

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



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

Conditions ⓘ

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 2400000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 1400000000"/>



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

Uma expressão básica é geralmente da forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

O padrão é 5 minutos.

8. Selecione **Guardar**.

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

Desativar regras de alerta

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Sobre esta tarefa

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



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

Passos

1. Selecione **ALERTAS > regras**.

A página regras de alerta é exibida.

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

A caixa de diálogo Editar regra é exibida.

4. Marque ou desmarque a caixa de seleção **Enabled** para determinar se essa regra de alerta está ativada

no momento.

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



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

5. Selecione **Guardar**.

Disabled aparece na coluna **Status**.

Remover regras de alerta personalizadas

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Passos

1. Selecione **ALERTAS > regras**.

A página regras de alerta é exibida.

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

Não é possível remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

É apresentada uma caixa de diálogo de confirmação.

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

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

Gerenciar notificações de alerta

Configurar notificações SNMP para alertas

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

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

Para saber como configurar o agente SNMP, ["Utilize a monitorização SNMP"](#) consulte .

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

ser enviados:

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

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

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

Configurar notificações por e-mail para alertas

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Sobre esta tarefa

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

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

Passos

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

A página Configuração de e-mail é exibida.

Email Setup

You can configure the email server for alert notifications, define filters to limit the number of notifications, and enter email addresses for alert recipients.

Use these settings to define the email server used for alert notifications. These settings are not used for alarm notifications and AutoSupport. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Enable Email Notifications  ☐

Save

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

As seções servidor de e-mail (SMTP), TLS (Transport Layer Security), endereços de e-mail e filtros são exibidas.

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

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

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

Email (SMTP) Server

Mail Server 	<input type="text" value="10.224.1.250"/>
Port 	<input type="text" value="25"/>
Username (optional) 	<input type="text" value="smtpuser"/>
Password (optional) 	<input type="password" value="*****"/>

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

Por exemplo: storagegrid-alerts@example.com

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

Selecione o ícone de mais **+** para adicionar destinatários.

Email Addresses

Sender Email Address ?	<input type="text" value="storagegrid-alerts@example.com"/>	
Recipient 1 ?	<input type="text" value="recipient1@example.com"/>	✕
Recipient 2 ?	<input type="text" value="recipient2@example.com"/>	+ ✕

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

- a. No campo **certificado CA**, forneça o certificado CA que será usado para verificar a identificação do servidor SMTP.

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

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

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

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


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


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




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


Transport Layer Security (TLS)

Require TLS  ☒


CA Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Send Client Certificate  ☒

Client Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Private Key 

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----BEGIN PRIVATE KEY-----
```

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

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

Gravidade	Descrição
Apenas crítica	Uma notificação por e-mail é enviada somente quando a condição crítica de uma regra de alerta é atendida. As notificações não são enviadas para alertas menores ou maiores.

Filters

Severity ?

☒ Minor, major, critical

☐ Major, critical

☐ Critical only

Send Test Email

Save

7. Quando estiver pronto para testar suas configurações de e-mail, execute estas etapas:

a. Selecione **Enviar e-mail de teste**.

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

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



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

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



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

8. Selecione **Guardar**.

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

As configurações de e-mail são salvas.

Informações incluídas nas notificações por e-mail de alerta

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

As notificações por e-mail incluem as seguintes informações:

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 5

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

Como os alertas são agrupados

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

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

Comportamento	Exemplo
Cada notificação de alerta aplica-se apenas a alertas com o mesmo nome. Se dois alertas com nomes diferentes forem acionados ao mesmo tempo, duas notificações por e-mail serão enviadas.	<ul style="list-style-type: none"> • O alerta A é acionado em dois nós ao mesmo tempo. Apenas uma notificação é enviada. • O alerta A é acionado no nó 1 e o alerta B é acionado no nó 2 ao mesmo tempo. Duas notificações são enviadas - uma para cada alerta.
Para um alerta específico em um nó específico, se os limites forem atingidos por mais de uma gravidade, uma notificação será enviada apenas para o alerta mais grave.	<ul style="list-style-type: none"> • O alerta A é acionado e os limites de alerta menor, maior e crítico são atingidos. Uma notificação é enviada para o alerta crítico.
Na primeira vez que um alerta é acionado, o StorageGRID aguarda 2 minutos antes de enviar uma notificação. Se outros alertas com o mesmo nome forem acionados durante esse período, o StorageGRID agrupa todos os alertas na notificação inicial.	<ol style="list-style-type: none"> 1. O alerta A é acionado no nó 1 às 08:00. Nenhuma notificação é enviada. 2. O alerta A é acionado no nó 2 às 08:01. Nenhuma notificação é enviada. 3. Às 08:02, uma notificação é enviada para relatar ambas as instâncias do alerta.
Se um outro alerta com o mesmo nome for acionado, o StorageGRID aguarda 10 minutos antes de enviar uma nova notificação. A nova notificação relata todos os alertas ativos (alertas atuais que não foram silenciados), mesmo que tenham sido reportados anteriormente.	<ol style="list-style-type: none"> 1. O alerta A é acionado no nó 1 às 08:00. Uma notificação é enviada às 08:02. 2. O alerta A é acionado no nó 2 às 08:05. Uma segunda notificação é enviada às 08:15 (10 minutos depois). Ambos os nós são relatados.
Se houver vários alertas atuais com o mesmo nome e um desses alertas for resolvido, uma nova notificação não será enviada se o alerta ocorrer novamente no nó para o qual o alerta foi resolvido.	<ol style="list-style-type: none"> 1. O alerta A é acionado para o nó 1. Uma notificação é enviada. 2. O alerta A é acionado para o nó 2. Uma segunda notificação é enviada. 3. O alerta A foi resolvido para o nó 2, mas permanece ativo para o nó 1. 4. O alerta A é acionado novamente para o nó 2. Nenhuma nova notificação é enviada porque o alerta ainda está ativo para o nó 1.
O StorageGRID continua a enviar notificações por e-mail uma vez a cada 7 dias até que todas as instâncias do alerta sejam resolvidas ou a regra de alerta seja silenciada.	<ol style="list-style-type: none"> 1. O alerta A é acionado para o nó 1 em 8 de março. Uma notificação é enviada. 2. O alerta A não foi resolvido ou silenciado. Notificações adicionais são enviadas em 15 de março, 22 de março, 29 de março, e assim por diante.

Solucionar problemas de notificações por e-mail de alerta

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Passos

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

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

["Colete arquivos de log e dados do sistema"](#)Consulte .

Silenciar notificações de alerta

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Gerencie alertas ou permissão de acesso root"](#).

Sobre esta tarefa

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

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



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



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

Passos

1. Selecione **ALERTAS > silêncios**.

É apresentada a página silêncios.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

Create

Edit

Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Selecione **criar**.

A caixa de diálogo criar Silêncio é exibida.

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

☐ Minor only

☐ Minor, major

☐ Minor, major, critical

Nodes

☐ StorageGRID Deployment

☐ Data Center 1

☐ DC1-ADM1

☐ DC1-G1

☐ DC1-S1

☐ DC1-S2

☐ DC1-S3

Cancel

Save

3. Selecione ou introduza as seguintes informações:

Campo	Descrição
Regra de alerta	<p>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.</p> <p>Observação: Selecione todas as regras se quiser silenciar todas as regras de alerta usando os critérios especificados nesta caixa de diálogo.</p>

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

4. Selecione **Guardar**.

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

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

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

Informações relacionadas

- ["Configure o agente SNMP"](#)

Referência de alertas

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

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

Alguns dos alertas padrão usam ["Métricas Prometheus"](#)o .

Alertas de dispositivo

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

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

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

Nome do alerta	Descrição
Falha na fonte de alimentação B do controlador de armazenamento do dispositivo	A fonte de alimentação B num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.
O serviço de monitor de hardware de armazenamento do dispositivo parou	O serviço que monitora o status do hardware de storage parou.
Prateleiras de storage do dispositivo degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento é degradado.
Temperatura do aparelho excedida	A temperatura nominal ou máxima para o controlador de armazenamento do aparelho foi excedida.
Sensor de temperatura do aparelho removido	Um sensor de temperatura foi removido.
Erro de inicialização segura UEFI do appliance	Um aparelho não foi inicializado com segurança.
A e/S do disco é muito lenta	E/S de disco muito lento pode estar impactando o desempenho da grade.
Detectada avaria na ventoinha do aparelho de armazenamento	Foi detetado um problema com um ventilador no controlador de armazenamento de um aparelho.
Conectividade de storage do dispositivo de storage degradada	Há um problema com uma ou mais conexões entre o controlador de computação e o controlador de storage.
Dispositivo de armazenamento inacessível	Não é possível aceder a um dispositivo de armazenamento.

Alertas de auditoria e syslog

Nome do alerta	Descrição
Os logs de auditoria estão sendo adicionados à fila na memória	O nó não pode enviar logs para o servidor syslog local e a fila na memória está sendo preenchida.
Erro de encaminhamento do servidor syslog externo	O nó não pode encaminhar logs para o servidor syslog externo.
Fila de auditoria grande	A fila de discos para mensagens de auditoria está cheia. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.

Nome do alerta	Descrição
Os logs estão sendo adicionados à fila no disco	O nó não pode encaminhar logs para o servidor syslog externo e a fila no disco está sendo preenchida.

Alertas de intervalo

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

Alertas do Cassandra

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

Alertas do Cloud Storage Pool

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

Alertas de replicação entre grades

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

Alertas DHCP

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

Depurar e rastrear alertas

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

Alertas de e-mail e AutoSupport

Nome do alerta	Descrição
Falha ao enviar a mensagem AutoSupport	Não foi possível enviar a mensagem AutoSupport mais recente.
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail para um alerta.

Alertas de codificação de apagamento (EC)

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

Expiração de alertas de certificados

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

Alertas da rede de grelha

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

Alertas de federação de grade

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

Alertas de alta utilização ou alta latência

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

Alertas de federação de identidade

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

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

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

Alertas de servidor de gerenciamento de chaves (KMS)

Nome do alerta	Descrição
Expiração do certificado CA de KMS	O certificado de autoridade de certificação (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Expiração do certificado do cliente KMS	O certificado de cliente para um servidor de gerenciamento de chaves está prestes a expirar
Falha ao carregar a configuração DE KMS	A configuração para o servidor de gerenciamento de chaves existe, mas não foi possível carregar.
Erro de conectividade DE KMS	Um nó de dispositivo não pôde se conectar ao servidor de gerenciamento de chaves para seu site.
Nome da chave de encriptação KMS não encontrado	O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido.
Falha na rotação da chave de CRIPTOGRAFIA KMS	Todos os volumes de dispositivos foram descriptografados com êxito, mas um ou mais volumes não puderam girar para a chave mais recente.
KMS não está configurado	Não existe nenhum servidor de gerenciamento de chaves para este site.
A chave KMS falhou ao descriptar um volume de aparelho	Um ou mais volumes em um dispositivo com criptografia de nó ativada não puderam ser descriptografados com a chave KMS atual.
Expiração do certificado do servidor DE KMS	O certificado do servidor usado pelo KMS (Key Management Server) está prestes a expirar.

Alertas de desvio do relógio local

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

Alertas de memória baixa ou de espaço reduzido

Nome do alerta	Descrição
Baixa capacidade de disco de log de auditoria	O espaço disponível para logs de auditoria é baixo. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Baixa memória disponível do nó	A quantidade de RAM disponível em um nó é baixa.

Nome do alerta	Descrição
Baixo espaço livre para piscina de armazenamento	O espaço disponível para armazenar dados de objetos no nó de armazenamento é baixo.
Baixa memória do nó instalada	A quantidade de memória instalada em um nó é baixa.
Baixo armazenamento de metadados	O espaço disponível para armazenar metadados de objetos é baixo.
Baixa capacidade de disco de métricas	O espaço disponível para o banco de dados de métricas é baixo.
Baixo armazenamento de dados de objetos	O espaço disponível para armazenar dados de objetos é baixo.
Baixa sobreposição de marca d'água somente leitura	A Sobreposição da marca d'água apenas de leitura suave do volume de armazenamento é inferior à marca d'água mínima otimizada para um nó de armazenamento.
Baixa capacidade de disco raiz	O espaço disponível no disco raiz é baixo.
Baixa capacidade de dados do sistema	O espaço disponível para /var/local é baixo. Se esta condição não for resolvida, as operações S3 ou Swift podem falhar.
Espaço livre do diretório de baixa tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de rede de nós ou nós

Nome do alerta	Descrição
Admin Network receber uso	O uso de recepção na rede Admin é alto.
Utilização de transmissão de rede Admin	A utilização de transmissão na rede de administração é elevada.
Falha na configuração do firewall	Falha ao aplicar a configuração da firewall.
Endpoints de interface de gerenciamento no modo fallback	Todos os endpoints de interface de gerenciamento têm voltado para as portas padrão por muito tempo.
Erro de conectividade de rede do nó	Ocorreram erros durante a transferência de dados entre nós.
Erro de quadro de recepção de rede do nó	Uma alta porcentagem dos quadros de rede recebidos por um nó teve erros.

Nome do alerta	Descrição
Nó não sincronizado com o servidor NTP	O nó não está em sincronia com o servidor NTP (Network Time Protocol).
Nó não bloqueado com servidor NTP	O nó não está bloqueado para um servidor NTP (Network Time Protocol).
Rede de nós que não são do dispositivo inativa	Um ou mais dispositivos de rede estão inativos ou desconetados.
Link do utilitário de serviços para baixo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do utilitário de serviços para baixo na porta de rede Admin 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.
Link do utilitário de serviços para baixo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Link do dispositivo de serviços para baixo na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.
Link do dispositivo de armazenamento na rede Admin	A interface do dispositivo para a rede de administração (eth1) está inativa ou desligada.
Link do dispositivo de armazenamento na porta Admin Network 1	A porta Admin Network 1 do aparelho está inativa ou desconetada.
Ligação do dispositivo de armazenamento na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 1	A porta de rede 1 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 2	A porta de rede 2 do aparelho está inativa ou desligada.

Nome do alerta	Descrição
Ligação do dispositivo de armazenamento na porta de rede 3	A porta de rede 3 do aparelho está inativa ou desligada.
Ligação do dispositivo de armazenamento na porta de rede 4	A porta de rede 4 do aparelho está inativa ou desligada.
Nó de storage não no estado de storage desejado	O serviço LDR em um nó de armazenamento não pode fazer a transição para o estado desejado devido a um erro interno ou problema relacionado ao volume
Utilização da ligação TCP	O número de conexões TCP neste nó está se aproximando do número máximo que pode ser rastreado.
Não é possível comunicar com o nó	Um ou mais serviços não respondem ou o nó não pode ser alcançado.
Reinicialização inesperada do nó	Um nó reinicializou inesperadamente nas últimas 24 horas.

Alertas de objetos

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

Alertas de serviços de plataforma

Nome do alerta	Descrição
Capacidade de solicitação pendente de Serviços de Plataforma baixa	O número de solicitações pendentes de Serviços de Plataforma está se aproximando da capacidade.

Nome do alerta	Descrição
Serviços de plataforma indisponíveis	Poucos nós de storage com o serviço RSM estão em execução ou disponíveis em um local.

Alertas de volume de storage

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

Alertas dos serviços do StorageGRID

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

Alertas do locatário

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

Métricas de Prometheus comumente usadas

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

Você também [obtenha uma lista completa de todas as métricas](#) pode .

Para obter detalhes sobre a sintaxe das consultas Prometheus, "[Consultando Prometheus](#)" consulte .

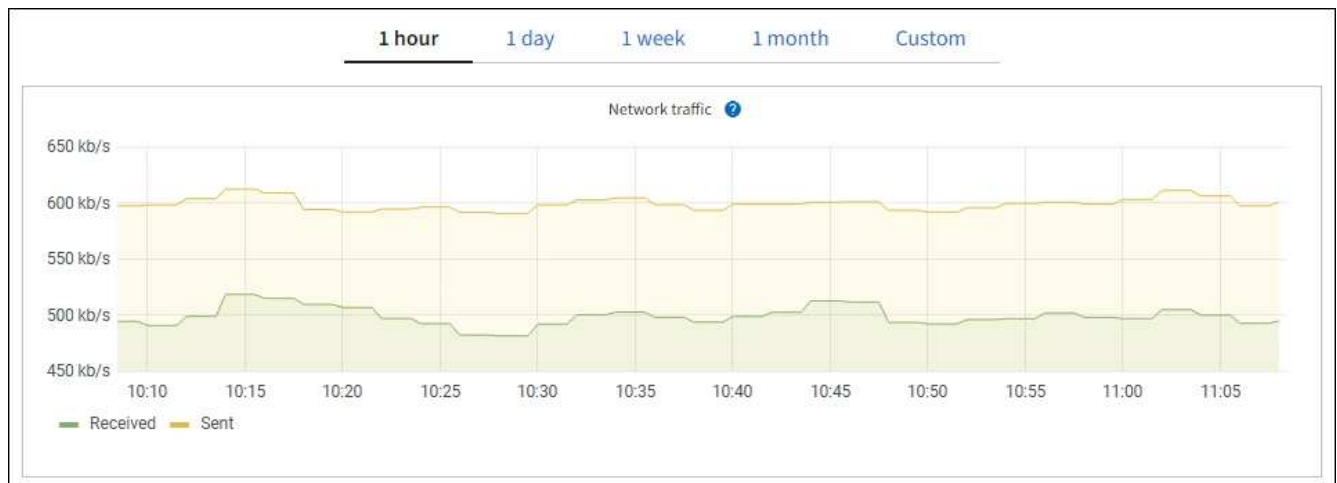
O que são métricas Prometheus?

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

Onde são usadas as métricas do Prometheus?

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

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



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



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

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



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

Lista das métricas mais comuns

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



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

alertmanager_notifications_failed_total

O número total de notificações de alerta com falha.

node_filesystem_avail_bytes

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

Node_Memory_MemAvailable_bytes

Campo de informações de memória MemAvailable_bytes.

node_network_carrier

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

node_network_receive_errs_total

Estatística do dispositivo de rede `receive_errs` .

node_network_transmit_errs_total

Estatística do dispositivo de rede `transmit_errs` .

StorageGRID_administrativamente_down

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

StorageGRID_appliance_compute_controller_hardware_status

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

StorageGRID_appliance_failed_disks

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

StorageGRID_appliance_storage_controller_hardware_status

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

StorageGRID_content_buckets_and_containers

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

StorageGRID_content_objects

O número total de objetos de dados S3 e Swift conhecido por este nó de storage. A contagem é válida

apenas para objetos de dados criados por aplicativos clientes que fazem interface com o sistema através de S3 ou Swift.

StorageGRID_content_objects_lost

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

["Solucionar problemas de dados de objetos perdidos e ausentes"](#)

StorageGRID_http_sessions_incoming_tented

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

StorageGRID_http_sessions_incoming_currently_established

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

StorageGRID_http_sessions_incoming_failed

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

StorageGRID_http_sessions_incoming_successful

O número total de sessões HTTP concluídas com êxito.

StorageGRID_ilm_awaiting_background_objects

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

StorageGRID_ilm_awaiting_client_evaluation_objects_per_second

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

StorageGRID_ilm_awaiting_client_objects

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

StorageGRID_ilm_awaiting_total_objects

O número total de objetos aguardando avaliação ILM.

StorageGRID_ilm_scan_objects_per_second

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

StorageGRID_ilm_scan_period_estimated_minutes

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

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

StorageGRID_load_balancer_endpoint_cert_expiry_time

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

StorageGRID_metadata_queries_average_latency_milésimos de segundo

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

StorageGRID_network_received_bytes

A quantidade total de dados recebidos desde a instalação.

StorageGRID_network_transmitted_bytes

A quantidade total de dados enviados desde a instalação.

StorageGRID_node_cpu_utilization_percentage

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

StorageGRID_ntp_chosen_time_source_offset_milissegundos

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

StorageGRID_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

O número total de operações S3 falhadas que resultam de uma falha de autorização.

StorageGRID_servercertificate_management_interface_cert_expiry_days

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

StorageGRID_servercertificate_storage_api_endpoints_cert_expiry_days

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

StorageGRID_service_cpu_seconds

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

StorageGRID_service_memory_usage_bytes

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

StorageGRID_service_network_received_bytes

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

StorageGRID_service_network_transmitted_bytes

A quantidade total de dados enviados por este serviço.

StorageGRID_service_restarts

O número total de vezes que o serviço foi reiniciado.

StorageGRID_service_runtime_seconds

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

StorageGRID_service_uptime_seconds

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

StorageGRID_storage_state_current

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

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

StorageGRID_storage_status

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

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

StorageGRID_storage_utilization_data_bytes

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

StorageGRID_storage_utilization_metadata_allowed_bytes

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

StorageGRID_storage_utilization_metadata_bytes

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

StorageGRID_storage_utilization_total_space_bytes

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

StorageGRID_storage_utilization_usable_space_bytes

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

StorageGRID_swift_data_transfers_bytes ingerido

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

StorageGRID_swift_data_transfers_bytes recuperados

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

StorageGRID_swift_operations_failed

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

StorageGRID_swift_operations_successful

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

StorageGRID_swift_operations_unauthorized

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

StorageGRID_tenant_usage_data_bytes

O tamanho lógico de todos os objetos para o locatário.

StorageGRID_tenant_use_object_count

O número de objetos para o inquilino.

StorageGRID_tenant_usage_quota_bytes

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

Obtenha uma lista de todas as métricas

para obter a lista completa de métricas, use a API Grid Management.

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

Gerenciar alarmes (sistema legado)

Gerenciar alarmes (sistema legado)

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



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





Classes de alarme (sistema legado)

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

- Os alarmes padrão são fornecidos com cada sistema StorageGRID e não podem ser modificados. No entanto, você pode desativar os alarmes padrão ou substituí-los definindo alarmes personalizados globais.
- Os alarmes personalizados globais monitoram o status de todos os serviços de um determinado tipo no sistema StorageGRID. Você pode criar um alarme personalizado global para substituir um alarme padrão. Você também pode criar um novo alarme Global Custom. Isso pode ser útil para monitorar quaisquer condições personalizadas do seu sistema StorageGRID.

Lógica de acionamento de alarme (sistema legado)

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

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

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

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

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

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

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

Exemplo de acionamento de alarmes

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

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

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

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

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

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

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








Alarmes da mesma gravidade

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

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



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		   
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		   

Se a ordem é invertida, quando UMEM cai para 100MB, o primeiro alarme (100000000) é acionado, mas não o abaixo dele (500000000).



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		   
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		   


Default Alarms

Filter by Disabled Defaults



0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes 

Notificações

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

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

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

alarme mostre o valor de gatilho como 2,0.

Novos serviços

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

Alarmes e tabelas

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

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

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

Volumes

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

Reconhecer alarmes atuais (sistema legado)

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

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você deve ter a permissão de reconhecer alarmes.

Sobre esta tarefa

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



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

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



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

Passos

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

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Current Alarmes

Last Refreshed: 2020-05-27 09:41:39 MDT

☐ Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show 50 Records Per Page Refresh Previous 1 Next

2. Selecione o nome do serviço na tabela.

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

Overview


Alarms

Reports


Configuration

Main

History

 **Alarms: ARC (DC1-ARC1) - Replication**
Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes 

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

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



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

4. Conforme necessário, visualize os alarmes reconhecidos.
 - a. Selecione **SUPPORT > Alarmes (legacy) > Current Alarmes**.
 - b. Selecione **Mostrar alarmes confirmados**.

São apresentados quaisquer alarmes reconhecidos.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 17:38:58 MDT

☒ Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable	2020-05-27 17:38:14 MDT

Show 50 Records Per Page Refresh Previous 1 Next

Exibir alarmes padrão (sistema legado)

Pode ver a lista de todos os alarmes herdados predefinidos.

Antes de começar

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



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

Passos

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

Todos os alarmes predefinidos estão listados.



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
<input checked="" type="checkbox"/>		XCVP (% Completion)	Notice	Foreground Verification Completed	=	100	
<input checked="" type="checkbox"/>	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
<input checked="" type="checkbox"/>	ADC	ADCE (ADC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
<input checked="" type="checkbox"/>	ADC	ALOS (Outbound Attribute Sessions)	Notice	Over 200	>=	200	

Rever alarmes históricos e frequência de alarmes (sistema legado)

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

Antes de começar

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



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

Passos

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

2. Siga estas etapas para descobrir a frequência com que alarmes foram acionados para um atributo específico.
 - a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Selecione **grid node > Service ou Component > Alarmes > History**.
 - c. Selecione o atributo na lista.
 - d. Execute um dos seguintes procedimentos:
 - Clique num dos períodos de tempo.
 - Insira um intervalo personalizado e clique em **consulta personalizada**.
- Os alarmes são listados em ordem cronológica inversa.
- e. Para retornar ao formulário de solicitação do histórico de alarmes, clique em **Histórico**.

Criar alarmes personalizados globais (sistema legado)

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

Antes de começar

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





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

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



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

Passos

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






Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10		   
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		   
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000		   

Default Alarms

Filter by Attribute Code equals AR* 

9 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10	 
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	 
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	 
<input checked="" type="checkbox"/>	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	 
<input checked="" type="checkbox"/>	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	 
<input checked="" type="checkbox"/>	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	 
<input checked="" type="checkbox"/>	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	 
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	 
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Notice	Standby	<=	19	 

Apply Changes 

- Para modificar um alarme predefinido, procure o alarme predefinido.

- i. Em Filtrar por, selecione **Código Atributo** ou **Nome Atributo**.

- ii. Digite uma string de pesquisa.

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







- iii. Clique na seta  ou pressione **Enter**.

- iv. Na lista de resultados, clique em **Copiar**  ao lado do alarme que deseja modificar.

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

- Faça as alterações necessárias às definições de alarmes personalizados globais:

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

Rumo	Descrição
Atributo	Selecione o nome e o código do atributo que está sendo monitorado na lista de todos os atributos aplicáveis ao serviço ou componente selecionado. Para exibir informações sobre o atributo, clique em Info  ao lado do nome do atributo.
Gravidade	O ícone e o texto que indicam o nível do alarme.
Mensagem	O motivo do alarme (perda de conexão, espaço de armazenamento abaixo de 10%, e assim por diante).
Operador	Operadores para testar o valor do atributo atual em relação ao limite do valor: <ul style="list-style-type: none"> • igual a • > superior a. • inferior a. • > superior ou igual a • menos ou igual a • ≠ não é igual a
Valor	O valor limite do alarme usado para testar o valor real do atributo usando o operador. A entrada pode ser um único número, um intervalo de números especificado com dois pontos (1:3) ou uma lista delimitada por vírgulas de números e intervalos.
Destinatários adicionais	Uma lista suplementar de endereços de e-mail a notificar quando o alarme é acionado. Isso é além da lista de e-mails configurada na página Alarmes > Configuração de e-mail . As listas são delineadas por vírgulas. Observação: listas de discussão exigem configuração do servidor SMTP para operar. Antes de adicionar listas de discussão, confirme se o SMTP está configurado. As notificações de alarmes personalizados podem substituir as notificações de alarmes personalizados globais ou predefinidos.
Ações	Botões de controle para:  Editar uma linha  Insira uma linha  Elimine uma linha  Arraste uma linha para cima ou para baixo  Copie uma linha

4. Clique em **aplicar alterações**.

Desativar alarmes (sistema legado)

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



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

Desativar um alarme predefinido (sistema legado)

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

Antes de começar

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

Sobre esta tarefa

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



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

Passos

1. Selecione **SUPPORT > Alarmes (legacy) > Alarmes globais**.
2. Procure o alarme predefinido para desativar.


- a. Na seção Alarmes padrão, selecione **Filtrar por > Código de Atributo** ou **Nome do Atributo**.
- b. Digite uma string de pesquisa.

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

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






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

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












Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								   

Default Alarms

Filter by equals 

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	 Critical	Under 10000000	<=	10000000	 
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	 Major	Under 50000000	<=	50000000	 
<input type="checkbox"/>	SSM	UMEM (Available Memory)	 Minor	Under 100000000	<=	100000000	 

Apply Changes 

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

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

O alarme predefinido está desativado.

Desativar alarmes personalizados globais (sistema legado)

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


Antes de começar

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

Sobre esta tarefa

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

Passos

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



Global Custom Alarms (1 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>	All	RDTE (Tivoli Storage Manager State)	Major	Offline	=	10		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

4. Clique em **aplicar alterações**.

O alarme personalizado global está desativado.

Apagar alarmes acionados (sistema legado)

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

Antes de começar

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

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

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

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

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

O alarme é apagado.

Configurar notificações para alarmes (sistema legado)

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

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

Tipos de notificações de alarme (sistema legado)

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

Notificações de nível de gravidade

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

- Aviso
- Menor
- Maior
- Crítico

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

Notificações do estado do serviço

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

- Desconhecido
- Administrativamente para baixo

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

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

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

Antes de começar

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

Sobre esta tarefa

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



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

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

Passos

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

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

Use these settings to define the email server used for alarm notifications and for AutoSupport messages. These settings are not used for alert notifications. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).



Email Server

Updated: 2016-03-17 11:11:59 PDT

E-mail Server (SMTP) Information

Mail Server	<input type="text"/>
Port	<input type="text"/>
Authentication	<input type="button" value="Off"/>
Authentication Username	<input type="text" value="root"/>
Authentication Password	<input type="password" value="....."/>
From Address	<input type="text"/>
Test E-mail To	<input type="text"/>
<input type="checkbox"/> Send Test E-mail	

Apply Changes

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

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

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

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

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

- b. Selecione **Enviar e-mail de teste**.

6. Clique em **aplicar alterações**.

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

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

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

Antes de começar



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

Sobre esta tarefa

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

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

Passos

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



Template (0 - 0 of 0)

Template Name	Subject Prefix	Header	Footer	Actions
Template One	Notifications	All Email Lists	From SGWS	  

Show 50 Records Per Page

Refresh

« »

Apply Changes



4. Na nova linha, adicione o seguinte:

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

5. Clique em **aplicar alterações**.

Um novo modelo para notificações é adicionado.

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

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



Antes de começar

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

Sobre esta tarefa

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

Passos

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



Email Lists

Updated: 2016-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  
Show <input type="text" value="50"/> Records Per Page <input type="button" value="Refresh"/>			

Apply Changes 

4. Na nova linha, adicione o seguinte:

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

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

5. Clique em **aplicar alterações**.

Uma nova lista de discussão é criada.

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

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

Antes de começar



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

Sobre esta tarefa

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

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

Passos

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

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

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

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

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

Antes de começar


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

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



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

Passos

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

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

Ver alarmes legados

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



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

Antes de começar

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

Passos

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

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms





Last Refreshed: 2020-05-27 09:41:39 MDT

☐ Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page Previous « 1 » Next

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

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

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

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

Overview

Alarms

Reports

Configuration

Main

History

Alarms: ARC (DC1-ARC1) - Replication
 Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes

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

Informações relacionadas

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

["Reconhecer alarmes atuais \(sistema legado\)"](#)

["Desativar alarmes \(sistema legado\)"](#)

Referência de alarmes (sistema legado)

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



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

Código	Nome	Serviço	Ação recomendada
ABRL	Relés Atributo disponíveis	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>Restaure a conectividade a um serviço (um serviço ADC) executando um serviço de relé de atributos o mais rápido possível. Se não houver relés de atributos conectados, o nó de grade não poderá relatar valores de atributo ao serviço NMS. Assim, o serviço NMS não pode mais monitorar o status do serviço ou atualizar atributos para o serviço.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>

Código	Nome	Serviço	Ação recomendada
ACMS	Serviços de metadados disponíveis	BARC, BLDR, BCMN	<p>Um alarme é acionado quando um serviço LDR ou ARC perde a ligação a um serviço DDS. Se isso ocorrer, as transações de ingestão ou recuperação não podem ser processadas. Se a indisponibilidade dos serviços DDS for apenas um breve problema transitório, as transações podem ser atrasadas.</p> <p>Verifique e restaure as ligações a um serviço DDS para apagar este alarme e devolver o serviço à funcionalidade completa.</p>
ATUA	Status de serviço do Cloud Tiering	ARCO	<p>Disponível apenas para nós de arquivamento com um tipo de destino de disposição em camadas na nuvem - Simple Storage Service (S3).</p> <p>Se o atributo ACTS para o nó de arquivo estiver definido como somente leitura ativado ou leitura-escrita Desativado, você deverá definir o atributo como leitura-escrita habilitado.</p> <p>Se um alarme principal for acionado devido a uma falha de autenticação, verifique as credenciais associadas ao intervalo de destino e atualize os valores, se necessário.</p> <p>Se um alarme principal for acionado devido a qualquer outro motivo, contacte o suporte técnico.</p>
ADCA	Estado ADC	ADC	<p>Se um alarme for acionado, selecione SUPPORT > Tools > Grid topology. Em seguida, selecione site > grid node > ADC > Overview > Main e ADC > Alarmes > Main para determinar a causa do alarme.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
ADCE	Estado ADC	ADC	<p>Se o valor do Estado ADC for Standby, continue monitorando o serviço e, se o problema persistir, entre em Contato com o suporte técnico.</p> <p>Se o valor de ADC State for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.</p>

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

Código	Nome	Serviço	Ação recomendada
ALUR	Repositórios Atributo inalcançáveis	ADC	<p>Verifique a conectividade de rede com o serviço NMS para garantir que o serviço possa entrar em Contato com o repositório de atributos.</p> <p>Se este alarme for acionado e a conectividade de rede estiver boa, contacte o suporte técnico.</p>
AMQS	Mensagens de auditoria enfileiradas	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	<p>Se as mensagens de auditoria não puderem ser encaminhadas imediatamente para um reencaminhamento ou repositório de auditoria, as mensagens serão armazenadas em uma fila de discos. Se a fila de discos ficar cheia, podem ocorrer interrupções.</p> <p>Para permitir que você responda a tempo para evitar uma interrupção, os alarmes AMQS são acionados quando o número de mensagens na fila de discos atinge os seguintes limites:</p> <ul style="list-style-type: none"> • Aviso: Mais de 100.000 mensagens • Menor: Pelo menos 500.000 mensagens • Maior: Pelo menos 2.000.000 mensagens • Crítico: Pelo menos 5.000.000 mensagens <p>Se um alarme AMQS for acionado, verifique a carga no sistema - se houver um número significativo de transações, o alarme deve resolver-se ao longo do tempo. Neste caso, pode ignorar o alarme.</p> <p>Se o alarme persistir e aumentar a gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para erro ou Desativado. "Configurar mensagens de auditoria e destinos de log"Consulte .</p>

Código	Nome	Serviço	Ação recomendada
AOTE	Estado da loja	BARC	<p>Disponível apenas para nós de arquivo com um tipo de destino do Tivoli Storage Manager (TSM).</p> <p>Se o valor do Estado de armazenamento estiver a aguardar o destino, verifique o sistema de armazenamento de arquivos externo e certifique-se de que está a funcionar corretamente. Se o nó de arquivo tiver sido adicionado ao sistema StorageGRID, certifique-se de que a ligação do nó de arquivo ao sistema de armazenamento de arquivos externo visado está configurada corretamente.</p> <p>Se o valor de Estado da loja estiver offline, verifique o valor de Estado da loja. Corrija quaisquer problemas antes de mover o estado da loja de volta para Online.</p>
AOTU	Estado da loja	BARC	<p>Se o valor de Status da Loja for sessão perdida, verifique se o sistema de armazenamento de arquivos externo está conetado e on-line.</p> <p>Se o valor de Target Error (erro de destino), verifique se há erros no sistema de armazenamento de arquivos externo.</p> <p>Se o valor do Status da Loja for erro desconhecido, entre em Contato com o suporte técnico.</p>
APMS	Conetividade Multipath de armazenamento	SSM	<p>Se o alarme de estado de multipath aparecer como "degradado" (selecione SUPPORT > Tools > Grid topology, selecione site > grid node > SSM > Events), faça o seguinte:</p> <ol style="list-style-type: none"> 1. Conete ou substitua o cabo que não exibe nenhuma luz indicadora. 2. Aguarde de um a cinco minutos. <p>Não desligue o outro cabo até, pelo menos, cinco minutos depois de ligar o primeiro. Desconetar muito cedo pode fazer com que o volume raiz se torne somente leitura, o que requer que o hardware seja reiniciado.</p> <ol style="list-style-type: none"> 3. Retorne à página SSM > recursos e verifique se o status do Multipath "degradado" foi alterado para "nominal" na seção hardware de armazenamento.

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

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

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

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

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

Código	Nome	Serviço	Ação recomendada
CASA	Estado do armazenamento de dados	DDS	<p>Um alarme é acionado se o armazenamento de metadados do Cassandra ficar indisponível.</p> <p>Verifique o status de Cassandra:</p> <ol style="list-style-type: none"> 1. No nó de armazenamento, faça login como administrador e su faça root usando a senha listada no arquivo Passwords.txt. 2. Introduza: <code>service cassandra status</code> 3. Se o Cassandra não estiver em execução, reinicie-o: <code>service cassandra restart</code> <p>Esse alarme também pode indicar que o armazenamento de metadados (banco de dados Cassandra) para um nó de armazenamento requer reconstrução.</p> <p>Consulte informações sobre como solucionar problemas do alarme Serviços: Status - Cassandra (SVST) no "Solucionar problemas de metadados".</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
CASO	Estado do armazenamento de dados	DDS	<p>Este alarme é acionado durante a instalação ou expansão para indicar que um novo armazenamento de dados está a aderir à grelha.</p>
CCNA	Hardware de computação	SSM	<p>Esse alarme é acionado se o status do hardware do controlador de computação em um dispositivo StorageGRID precisar de atenção.</p>

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

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

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

Código	Nome	Serviço	Ação recomendada
HSTU	Estado HTTP	ERRO	<p>HSTE e HSTU estão relacionados a HTTP para todo o tráfego LDR, incluindo S3, Swift, e outro tráfego StorageGRID interno. Um alarme indica que ocorreu uma das seguintes situações:</p> <ul style="list-style-type: none"> • O HTTP foi colocado offline manualmente. • O atributo Auto-Start HTTP foi desativado. • O serviço LDR está a encerrar. <p>O atributo Auto-Start HTTP é ativado por padrão. Se essa configuração for alterada, o HTTP poderá permanecer offline após uma reinicialização.</p> <p>Se necessário, aguarde que o serviço LDR seja reiniciado.</p> <p>Selecione SUPPORT > Tools > Grid topology. Em seguida, selecione Storage Node > LDR > Configuration. Se o HTTP estiver offline, coloque-o online. Verifique se o atributo Auto-Start HTTP está ativado.</p> <p>Se o HTTP permanecer offline, entre em Contato com o suporte técnico.</p>
HTAS	Auto-Iniciar HTTP	LDR	<p>Especifica se os serviços HTTP devem ser iniciados automaticamente na inicialização. Esta é uma opção de configuração especificada pelo usuário.</p>
IRSU	Estado de replicação de entrada	BLDR, BARC	<p>Um alarme indica que a replicação de entrada foi desativada. Confirme as configurações: Selecione SUPPORT > Tools > Grid topology. Em seguida, selecione site > grid node > LDR > Replication > Configuration > Main.</p>

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

Código	Nome	Serviço	Ação recomendada
MCEP	Validade do certificado de Interface de Gestão	CMN	<p>Acionado quando o certificado usado para acessar a interface de gerenciamento está prestes a expirar.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione CONFIGURATION > Security > Certificates. 2. Na guia Global, selecione certificado de interface de gerenciamento. 3. "Carregue um novo certificado de interface de gerenciamento."
MINQ	Notificações de e-mail na fila	NMS	<p>Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta.</p> <p>"Configurar as definições do servidor de correio eletrônico para alarmes (sistema legado)"</p>
MIN	Estado das notificações por e-mail	BNMS	<p>Um alarme menor é acionado se o serviço NMS não conseguir se conectar ao servidor de e-mail. Verifique as conexões de rede dos servidores que hospedam o serviço NMS e o servidor de e-mail externo. Confirme também se a configuração do servidor de e-mail está correta.</p> <p>"Configurar as definições do servidor de correio eletrônico para alarmes (sistema legado)"</p>
SAUDADES	Estado do motor da interface NMS	BNMS	<p>Um alarme é acionado se o mecanismo de interface NMS no Admin Node que reúne e gera conteúdo da interface for desconectado do sistema. Verifique o Gerenciador do servidor para determinar se o aplicativo individual do servidor está inativo.</p>
NANG	Configuração de negociação automática de rede	SSM	<p>Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede.</p> <p>Uma definição incorreta pode ter um impacto grave no desempenho do sistema.</p>
NDUP	Configuração Duplex de rede	SSM	<p>Verifique a configuração do adaptador de rede. A configuração deve corresponder às preferências dos roteadores e switches de rede.</p> <p>Uma definição incorreta pode ter um impacto grave no desempenho do sistema.</p>

Código	Nome	Serviço	Ação recomendada
NLNK	Detecção de ligação de rede	SSM	<p>Verifique as conexões do cabo de rede na porta e no switch.</p> <p>Verifique as configurações do roteador, do switch e do adaptador de rede.</p> <p>Reinicie o servidor.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
NRER	Receber erros	SSM	<p>As seguintes causas podem ser os alarmes NRER:</p> <ul style="list-style-type: none"> • Correção de erro de avanço (FEC) não corresponde • Incompatibilidade da MTU da porta do switch e da NIC • Altas taxas de erro de link • Buffer de anel NIC excedido <p>Consulte as informações sobre como solucionar problemas do alarme Network Receive Error (NRER) em "Solucionar problemas de rede, hardware e plataforma".</p>
NRLY	Relés de auditoria disponíveis	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	<p>Se os relés de auditoria não estiverem conectados aos serviços ADC, os eventos de auditoria não poderão ser relatados. Eles estão em fila de espera e indisponíveis para os usuários até que a conexão seja restaurada.</p> <p>Restaure a conectividade a um serviço ADC o mais rápido possível.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
NSCA	Estado NMS	NMS	<p>Se o valor de Status do NMS for DB Connectivity Error (erro de conectividade de banco de dados), reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.</p>
NSCE	Estado NMS	NMS	<p>Se o valor do estado NMS for Standby (espera), continue a monitorização e, se o problema persistir, contacte o suporte técnico.</p> <p>Se o valor de Estado NMS for Offline, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.</p>

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

Código	Nome	Serviço	Ação recomendada
NTSJ	Jitter de fonte de tempo escolhido	SSM	<p>Este valor indica a confiabilidade e estabilidade da fonte de tempo que o NTP no servidor local está usando como referência.</p> <p>Se um alarme for acionado, pode ser uma indicação de que o oscilador da fonte de tempo está com defeito ou que há um problema com o link WAN para a fonte de tempo.</p>
NTSU	Estado NTP	SSM	<p>Se o valor do Status NTP não estiver em execução, entre em Contato com o suporte técnico.</p>
OPST	Estado geral da alimentação	SSM	<p>Um alarme é acionado se a alimentação de um aparelho StorageGRID se desviar da tensão de funcionamento recomendada.</p> <p>Verifique o estado da fonte de Alimentação A ou B para determinar qual fonte de alimentação está a funcionar de forma anormal.</p> <p>Se necessário, substitua a fonte de alimentação.</p>
OQRT	Objetos em quarentena	LDR	<p>Depois que os objetos são restaurados automaticamente pelo sistema StorageGRID, os objetos em quarentena podem ser removidos do diretório de quarentena.</p> <ol style="list-style-type: none"> 1. Selecione SUPPORT > Tools > Grid topology. 2. Selecione site > nó de armazenamento > LDR > Verificação > Configuração > Principal. 3. Selecione Excluir objetos em quarentena. 4. Clique em aplicar alterações. <p>Os objetos em quarentena são removidos e a contagem é redefinida para zero.</p>
ORSU	Estado replicação saída	BLDR, BARC	<p>Um alarme indica que a replicação de saída não é possível: O armazenamento está em um estado em que os objetos não podem ser recuperados. Um alarme é acionado se a replicação de saída for desativada manualmente. Selecione SUPPORT > Tools > Grid topology. Em seguida, selecione site > grid node > LDR > Replication > Configuration.</p> <p>Um alarme é acionado se o serviço LDR não estiver disponível para replicação. Selecione SUPPORT > Tools > Grid topology. Em seguida, selecione site > grid node > LDR > Storage.</p>

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

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

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

Código	Nome	Serviço	Ação recomendada
SCEP	Validade do certificado de Endpoints do Serviço de API de armazenamento	CMN	<p>Acionado quando o certificado usado para acessar endpoints de API de armazenamento está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Selecione CONFIGURATION > Security > Certificates. 2. Na guia Global, selecione S3 e Swift API certificate. 3. "Faça upload de um novo certificado API S3 e Swift."
SCHR	Estado	CMN	<p>Se o valor de Status para a tarefa de grade histórica for abortado, investigue o motivo e execute a tarefa novamente, se necessário.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
SCSA	Controlador de armazenamento A	SSM	<p>Um alarme é acionado se houver um problema com o controlador de armazenamento A em um dispositivo StorageGRID.</p> <p>Se necessário, substituir o órgão.</p>
SCSB	Controlador de armazenamento B	SSM	<p>Um alarme é acionado se houver um problema com o controlador de armazenamento B em um dispositivo StorageGRID.</p> <p>Se necessário, substituir o órgão.</p> <p>Alguns modelos de aparelhos não têm um controlador de armazenamento B..</p>
SHLH	Saúde	LDR	<p>Se o valor de integridade para um armazenamento de objetos for erro, verifique e corrija:</p> <ul style="list-style-type: none"> • problemas com o volume a ser montado • erros do sistema de arquivos

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

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

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

Código	Nome	Serviço	Ação recomendada
SVST	Estado	SSM	<p>Este alarme é apagado quando outros alarmes relacionados a um serviço que não está em execução são resolvidos. Acompanhe os alarmes de serviço de origem para restaurar a operação.</p> <p>Selecione SUPPORT > Tools > Grid topology. Em seguida, selecione síte > grid node > SSM > Serviços > Visão geral > Principal. Quando o status de um serviço é mostrado como não em execução, seu estado é administrativamente inativo. O status do serviço pode ser listado como não em execução pelos seguintes motivos:</p> <ul style="list-style-type: none"> • O serviço foi interrompido manualmente (/etc/init.d/<service> stop). • Há um problema com o banco de dados MySQL e o Server Manager desliga o serviço MI. • Um nó de grade foi adicionado, mas não iniciado. • Durante a instalação, um nó de grade ainda não se conectou ao nó Admin. <p>Se um serviço estiver listado como não em execução, reinicie o serviço (/etc/init.d/<service> restart).</p> <p>Esse alarme também pode indicar que o armazenamento de metadados (banco de dados Cassandra) para um nó de armazenamento requer reconstrução.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p> <p>"Solucionar problemas do alarme Serviços: Status - Cassandra (SVST)"</p>
TMEM	Memória instalada	SSM	<p>Os nós executados com menos de 24 GiB de memória instalada podem levar a problemas de performance e instabilidade do sistema. A quantidade de memória instalada no sistema deve ser aumentada para pelo menos 24 GiB.</p>
TPOP	Operações pendentes	ADC	<p>Uma fila de mensagens pode indicar que o serviço ADC está sobrecarregado. Poucos serviços ADC podem ser conectados ao sistema StorageGRID. Em uma grande implantação, o serviço ADC pode exigir a adição de recursos computacionais, ou o sistema pode exigir serviços ADC adicionais.</p>

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

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

Referência de ficheiros de registo

Referência de ficheiros de registo: Visão geral

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

Os logs são categorizados da seguinte forma:

- ["Registos do software StorageGRID"](#)
- ["Logs de implantação e manutenção"](#)
- ["Logs para software de terceiros"](#)
- ["Sobre o bycast.log"](#)



Os detalhes fornecidos para cada tipo de log são apenas para referência. Os registros destinam-se à resolução de problemas avançada por suporte técnico. Técnicas avançadas que envolvem a reconstrução do histórico de problemas usando os logs de auditoria e os arquivos de log do aplicativo estão além do escopo dessas instruções.

Aceder aos registos

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

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

Categorias de ficheiros de registo

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

Localização do arquivo	Descrição
auditoria	Mensagens de auditoria geradas durante a operação normal do sistema.

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

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

Registos do software StorageGRID

Você pode usar logs do StorageGRID para solucionar problemas.



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

Registos gerais do StorageGRID

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

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

Registos relacionados com cifras

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

Logs de federação de grade

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

Registos NMS

Nome do ficheiro	Notas	Encontrado em
/var/local/log/nms.log	<ul style="list-style-type: none"> • Captura notificações do Grid Manager e do Tenant Manager. • Captura eventos relacionados à operação do serviço NMS, por exemplo, processamento de alarmes, notificações por e-mail e alterações de configuração. • Contém atualizações de pacotes XML resultantes de alterações de configuração feitas no sistema. • Contém mensagens de erro relacionadas ao atributo downsampling feito uma vez por dia. • Contém mensagens de erro do servidor Web Java, por exemplo, erros de geração de página e erros HTTP Status 500. 	Nós de administração
/var/local/log/nms.errlog	<p>Contém mensagens de erro relacionadas às atualizações do banco de dados MySQL.</p> <p>Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.</p>	Nós de administração
/var/local/log/nms.requestlog	Contém informações sobre conexões de saída da API de gerenciamento para serviços internos do StorageGRID.	Nós de administração

Logs do Server Manager

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

Registos de serviços do StorageGRID

Nome do ficheiro	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de storage executando o serviço ADC
/var/local/log/adc.errlog	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de storage executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/arc.errlog		Nós de arquivamento
/var/local/log/cassandra/system.log	Informações para o armazenamento de metadados (banco de dados Cassandra) que podem ser usadas se ocorrerem problemas ao adicionar novos nós de armazenamento ou se a tarefa de reparo nodetool for interrompida.	Nós de storage
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que executa reparos dos dados no banco de dados Cassandra.	Nós de storage
/var/local/log/cassandra-reaper.errlog	Informações de erro para o serviço Cassandra Reaper.	Nós de storage
/var/local/log/chunk.errlog		Nós de storage
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Esse arquivo de log pode estar presente em sistemas que foram atualizados a partir de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de storage
/var/local/log/cts.errlog	Esse arquivo de log só será criado se o tipo de destino for Cloud Tiering - Simple Storage Service (S3) .	Nós de arquivamento
/var/local/log/dds.errlog		Nós de storage

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/miscd/*.log	Contém logs para o serviço MISCD (Information Service Control Daemon), que fornece uma interface para consultar e gerenciar serviços em outros nós e para gerenciar configurações ambientais no nó, como consultar o estado dos serviços em execução em outros nós.	Todos os nós
/var/local/log/nginx/*.log	Contém logs para o serviço nginx, que atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e Dynip) para poder falar com serviços em outros nós através de APIs HTTPS.	Todos os nós
/var/local/log/nginx-gw/*.log	Contém logs gerais relacionados ao serviço nginx-gw, incluindo logs de erro e logs para as portas de administração restritas em nós de administração.	Nós de administração e nós de gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contém registros de acesso relacionados com o tráfego de replicação entre redes.	Nós de administração, nós de gateway ou ambos, com base na configuração da federação de grade. Apenas encontrado na grelha de destino para replicação entre grelhas.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contém logs de acesso para o serviço Load Balancer, que fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage.	Nós de administração e nós de gateway
/var/local/log/persistence*	Contém logs para o serviço Persistence, que gerencia arquivos no disco raiz que precisam persistir durante uma reinicialização.	Todos os nós
/var/local/log/prometheus.log	Para todos os nós, contém o log de serviço de exportador de nós e o log de serviço de métricas ade-exportador. For Admin node, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós

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

Informações relacionadas

["Sobre o bycast.log"](#)

["USE A API REST DO S3"](#)

Logs de implantação e manutenção

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

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

Nome do ficheiro	Notas	Encontrado em
/var/local/log/expansion-progress.log	Criado durante operações de expansão. Contém um Registro dos eventos de expansão.	Nós de storage
/var/local/log/pa-move.log	Criado durante a execução <code>pa-move.sh</code> do script.	Nó de administração principal
/var/local/log/pa-move-new_pa.log	Criado durante a execução <code>pa-move.sh</code> do script.	Nó de administração principal
/var/local/log/pa-move-old_pa.log	Criado durante a execução <code>pa-move.sh</code> do script.	Nó de administração principal
/var/local/log/gdu-server.log	Criado pelo serviço GDU. Contém eventos relacionados aos procedimentos de provisionamento e manutenção gerenciados pelo nó de administração principal.	Nó de administração principal
/var/local/log/send_admin_hw.log	Criado durante a instalação. Contém informações de depuração relacionadas às comunicações de um nó com o nó de administração principal.	Todos os nós
/var/local/log/upgrade.log	Criado durante a atualização de software. Contém um registo dos eventos de atualização de software.	Todos os nós

Logs para software de terceiros

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

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

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

Sobre o bycast.log

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

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

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado. "[Configurar mensagens de auditoria e destinos de log](#)" Consulte .

Rotação de ficheiros para bycast.log

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

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

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

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



Se um arquivo de log tiver sido compactado, você não deve descompactá-lo para o mesmo local em que foi escrito. A descompressão do arquivo para o mesmo local pode interferir com os scripts de rotação de log.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado. "[Configurar mensagens de auditoria e destinos de log](#)" Consulte .

Informações relacionadas

["Colete arquivos de log e dados do sistema"](#)

Mensagens em bycast.log

As mensagens em `bycast.log` são escritas pelo ADE (Asynchronous Distributed Environment). ADE é o ambiente de tempo de execução usado pelos serviços de cada nó de grade.

Exemplo de mensagem ADE:

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

As mensagens ADE contêm as seguintes informações:

Segmento de mensagens	Valor no exemplo
ID de nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador da mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29,784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUUUUUUUU)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação do estado do volume 3 falhou com o motivo "TOUT"

Severidades da mensagem em bycast.log

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

Por exemplo:

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

Códigos de erro em `bycast.log`

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

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

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

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

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

Número de erro	Código de erro	Significado
022	EINVAL	Argumento inválido
023	ENFILE	Estouro da tabela de arquivos
024	EMFILE	Demasiados ficheiros abertos
025	ENOTTY	Não é uma máquina de escrever
026	ETXTBSY	Ficheiro de texto ocupado
027	EFBIG	Ficheiro demasiado grande
028	ENOSPC	Nenhum espaço restante no dispositivo
029	ESPIPE	Procura ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Demasiados links
032	EPIPE	Tubo quebrado
033	EDOM	Argumento de matemática fora de domínio do func
034	ERANGE	Resultado matemático não representável
035	EDEADLK	O bloqueio de recursos ocorreria
036	ENAMETOOLONG	Nome do ficheiro demasiado longo
037	ENOLCK	Não existem bloqueios de registo disponíveis
038	ENOSYS	Função não implementada
039	ENOTEMPTY	O diretório não está vazio
040	ELOOP	Muitos links simbólicos encontrados
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido

Número de erro	Código de erro	Significado
044	ECHRNG	Número do canal fora do intervalo
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Reposição do nível 3
048	ELNRNG	Número da ligação fora do intervalo
049	EUNATCH	Controlador de protocolo não anexado
050	ENOCSE	Nenhuma estrutura CSI disponível
051	EL2HLT	Nível 2 interrompido
052	EBADE	Troca inválida
053	EBADR	Descritor de solicitação inválido
054	EXFULL	Troca completa
055	ENOANO	Sem ânodo
056	EBADRQC	Código de pedido inválido
057	EBADSLT	Ranhura inválida
058		
059	EBFONT	Formato de arquivo de fonte incorreto
060	ENOSTR	Dispositivo não é um fluxo
061	ENODATA	Nenhum dado disponível
062	ETIME	O temporizador expirou
063	ENOSR	Recursos fora de fluxos
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado

Número de erro	Código de erro	Significado
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 no envio
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de Multihop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	EOVERFLOW	Valor demasiado grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em mau estado
078	EREMCHG	Endereço remoto alterado
079	ELIBACC	Não é possível acessar uma biblioteca compartilhada necessária
080	ELIBBAD	Acessando uma biblioteca compartilhada corrompida
081	ELIBSCN	
082	ELIBMAX	Tentando vincular em muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada do sistema interrompida deve ser reiniciada

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

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

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

Configurar destinos de mensagens de auditoria e de log

Considerações para usar um servidor syslog externo

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

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

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

Quando usar um servidor syslog externo

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

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



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



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

Como configurar um servidor syslog externo

Para saber como configurar um servidor syslog externo, ["Configurar mensagens de auditoria e servidor syslog externo"](#) consulte .

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

- **Certificados de CA do servidor:** Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo na codificação PEM. Se omitido, o certificado padrão da CA de grade será usado.
- **Certificado de cliente:** O certificado de cliente para autenticação para o servidor syslog externo na codificação PEM.
- **Chave privada do cliente:** Chave privada para o certificado do cliente na codificação PEM.



Se você usar um certificado de cliente, você também deve usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, você também deve fornecer a senha. Não há benefício significativo de segurança ao usar uma chave privada criptografada porque a chave e a senha devem ser armazenadas; usar uma chave privada não criptografada, se disponível, é recomendado para simplificar.

Como estimar o tamanho do servidor syslog externo

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

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

Use S3 operações por segundo em fórmulas de estimativa

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



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

Fórmulas de estimativa para logs de auditoria

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os valores padrão (todas as categorias definidas como normal, exceto

armazenamento, que está definido como erro):

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

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

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

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

Vamos usar P para representar a porcentagem de S3 operações que são puts, onde $0 \leq P \leq 1$ (assim, para uma carga de trabalho DE 100% PUT, P 1, e para uma carga de trabalho DE 100% GET, P 0).

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

Se você puder determinar valores para P e K, poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os padrões (todas as categorias definidas como normal, exceto armazenamento, que está definido como erro):

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

Por exemplo, se sua grade for dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é

de 50% puts, e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1.500 mensagens syslog por segundo e deve ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de aproximadamente 1 MB por segundo.

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para logs de auditoria assumem o uso de configurações de nível de auditoria padrão (todas as categorias definidas como normal, exceto armazenamento, que é definido como erro). Fórmulas detalhadas para estimar a taxa e o tamanho médio das mensagens de auditoria para configurações de nível de auditoria não padrão não estão disponíveis. No entanto, a tabela a seguir pode ser usada para fazer uma estimativa aproximada da taxa; você pode usar a fórmula de tamanho médio fornecida para logs de auditoria, mas esteja ciente de que é provável que isso resulte em uma estimativa excessiva porque as mensagens de auditoria "extra" são, em média, menores do que as mensagens de auditoria padrão.

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

Fórmulas de estimativa para eventos de segurança

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

Fórmulas de estimativa para logs de aplicativos

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de Registros de aplicativos que seu servidor syslog externo precisará lidar com as seguintes fórmulas:

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

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

Se você sabe mais sobre sua carga de trabalho, estimativas mais precisas são possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. Codificação de apagamento), a porcentagem de operações S3 que são puts (vs. Gets/other) e o tamanho médio, em bytes, dos S3 campos a seguir (abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

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

Exemplo de estimativas de dimensionamento

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

- Replicação
- Codificação de apagamento

Se você usar a replicação para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde $0 \leq P \leq 1$ (assim, para uma carga de trabalho DE 100% PUT, P 1 e para uma carga de trabalho DE 100% GET, P 0).

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

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

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

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1800 Registros de aplicativos por segundo e receberá (e normalmente armazenará) dados de aplicativos a uma taxa de 0,5 MB por segundo.

Se você usar codificação de apagamento para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde $0 \leq P \leq 1$ (assim, para uma carga de trabalho DE 100% PUT, P 1 e para uma carga de trabalho DE 100% GET, P 0).

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

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

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

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 2.250 Registros de aplicativos por segundo e deve ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar mensagens de auditoria e servidor syslog externo

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

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

Opcionalmente, você pode configurar um servidor syslog externo para salvar informações de auditoria remotamente. O uso de um servidor externo minimiza o impactos no desempenho do Registro de mensagens de auditoria sem reduzir a integridade dos dados de auditoria. Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. ["Considerações para servidor syslog externo"](#) Consulte para obter detalhes.

Antes de começar

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

Alterar os níveis de mensagens de auditoria

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

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



Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10,3 ou posterior. Se você usou inicialmente uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como normal.



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

Passos

1. Selecione **CONFIGURATION > Monitoring > Audit and syslog Server**.
2. Para cada categoria de mensagem de auditoria, selecione um nível de auditoria na lista suspensa:

Nível de auditoria	Descrição
Desligado	Nenhuma mensagem de auditoria da categoria é registrada.
Erro	Somente mensagens de erro são registradas - mensagens de auditoria para as quais o código de resultado não foi "bem-sucedido" (SUCCS).
Normal	As mensagens transacionais padrão são registradas - as mensagens listadas nestas instruções para a categoria.

Nível de auditoria	Descrição
Depurar	Obsoleto. Este nível comporta-se da mesma forma que o nível normal de auditoria.

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



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

3. Selecione **Guardar**.

Um banner verde indica que sua configuração foi salva.

Definir cabeçalhos de solicitação HTTP

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

Passos

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

Use um asterisco (*) **como curinga para corresponder a zero ou mais 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 sob o campo HTRH.



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

3. Selecione **Guardar**

Um banner verde indica que sua configuração foi salva.

Use um servidor syslog externo

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



Se você não quiser usar um servidor syslog externo, pule esta etapa e vá para [Selecione destinos de informações de auditoria](#).



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

Insira as informações do syslog

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

Passos

1. Na página servidor de auditoria e syslog, selecione **Configurar servidor syslog externo**. Ou, se tiver configurado anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

O assistente Configurar servidor syslog externo é exibido.

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

Recomenda-se a utilização de **TLS** ou **REL/TLS**. Você deve carregar um certificado de servidor para usar qualquer uma dessas opções. O uso de certificados ajuda a proteger as conexões entre a grade e o servidor syslog externo. Para obter mais informações, ["Gerenciar certificados de segurança"](#) consulte .

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



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

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

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

7. Selecione **continuar**.

Gerenciar o conteúdo do syslog

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

Passos

1. Para a etapa **Manage syslog Content** do assistente, selecione cada tipo de informação de auditoria que deseja enviar para o servidor syslog externo.

- * **Enviar logs de auditoria***: Envia eventos do StorageGRID e atividades do sistema
- * **Enviar eventos de segurança***: Envia eventos de segurança, como quando um usuário não autorizado tenta entrar ou um usuário faz login como root
- * **Enviar logs de aplicativos***: Envia arquivos de log úteis para solução de problemas, incluindo:
 - `broadcast-err.log`
 - `broadcast.log`
 - `jaeger.log`
 - `nms.log` (Somente nós de administração)
 - `prometheus.log`
 - `raft.log`
 - `hagroups.log`

Para obter informações sobre os logs do software StorageGRID, "[Registros do software StorageGRID](#)" consulte .

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

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

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

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

Gravidade	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de gravidade que quando foi registrada localmente no nó: <ul style="list-style-type: none">• Para logs de auditoria, a gravidade é "info".• Para eventos de segurança, os valores de gravidade são gerados pela distribuição Linux nos nós.• Para logs de aplicativos, as severidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA dá um valor de "info", enquanto parar intencionalmente o serviço SSM ou RSM dá um valor de "notice".
0	Emergência: O sistema não pode ser utilizado
1	Alerta: A ação deve ser tomada imediatamente

Gravidade	Descrição
2	Crítico: Condições críticas
3	Erro: Condições de erro
4	Aviso: Condições de aviso
5	Aviso: Condição normal, mas significativa
6	Informativo: Mensagens informativas
7	Debug: Mensagens no nível de depuração

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

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

Instalação	Descrição
Passagem	<p>Cada mensagem enviada para o syslog externo para ter o mesmo valor de instalação que quando foi registrada localmente no nó:</p> <ul style="list-style-type: none"> • Para logs de auditoria, a instalação enviada para o servidor syslog externo é "local7". • Para eventos de segurança, os valores das instalações são gerados pela distribuição linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação: <ul style="list-style-type: none"> ◦ <code>bcast.log</code>: usuário ou daemon ◦ <code>bcast-err.log</code>: usuário, daemon, local3 ou local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6
0	kern (mensagens do kernel)
1	utilizador (mensagens no nível do utilizador)
2	e-mail

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

3. Seleccione **continuar**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós da grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudá-lo a validar toda a infraestrutura de coleta de logs antes de se comprometer a enviar dados para o servidor syslog externo.



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

Passos

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

Um banner verde indica que a configuração foi salva.

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

Os resultados do teste aparecem continuamente na página até que você pare o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuam sendo enviadas para os destinos configurados anteriormente.

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

["Solucionar problemas de um servidor syslog externo"](#) Consulte para ajudá-lo a resolver quaisquer erros.

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



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

6. Selecione **Parar e terminar**.

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



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

Selecione destinos de informações de auditoria

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

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



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

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

Passos

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



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

Opção	Descrição
Somente nós locais (padrão)	<p>As mensagens de auditoria, os logs de eventos de segurança e os logs de aplicativos não são enviados para os nós de administração. Em vez disso, eles são salvos apenas nos nós que os geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas no <code>/var/local/log/localaudit.log</code>.</p> <p>Nota: O StorageGRID remove periodicamente logs locais em uma rotação para liberar espaço. Quando o arquivo de log de um nó atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado. O limite de rotação para o log é de 21 arquivos. Quando a versão 22nd do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó.</p>
Nós de administração/nós locais	<p>As mensagens de auditoria são enviadas para o log de auditoria nos nós de administração, e os logs de eventos de segurança e de aplicativos são armazenados nos nós que as geraram. As informações de auditoria são armazenadas nos seguintes arquivos:</p> <ul style="list-style-type: none">• Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code>• Todos os nós: O <code>/var/local/log/localaudit.log</code> arquivo está normalmente vazio ou ausente. Ele pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
Servidor syslog externo	<p>As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais (<code>/var/local/log/localaudit.log</code>). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.</p>

Opção	Descrição
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (/var/local/audit/export/audit.log) em nós de administração e as informações de auditoria são enviadas para o servidor syslog externo e salvas no nó local (/var/local/log/localaudit.log). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.

2. Selecione **Guardar**.

É apresentada uma mensagem de aviso.

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

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

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

Utilize a monitorização SNMP

Usar monitoramento SNMP: Visão geral

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

- ["Configure o agente SNMP"](#)
- ["Atualize o agente SNMP"](#)

Recursos

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



Veja ["Acesse arquivos MIB"](#) se você deseja baixar os arquivos MIB em seus nós de grade.

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

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

Armadilhas

Traps são notificações enviadas pelo agente SNMP que não requerem confirmação pelo sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu dentro do

StorageGRID, como um alerta sendo acionado.

Traps são suportados em todas as três versões do SNMP.

Informa

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

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de intercetação e informação são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP para um alerta, tem de ["configure um silêncio"](#)o alertar. As notificações de alerta são enviadas pelo ["Nó Admin. Remetente preferido"](#).

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

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



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

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas (OBTEN e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de caracteres da comunidade	Cadeia de caracteres da comunidade	Utilizador do modelo de segurança baseado no utilizador (USM)
Notificações (ARMADILHA e INFORMAÇÃO)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Utilizador USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.
- SNMPv3: O StorageGRID não suporta o modo de suporte de transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é AES.

Configure o agente SNMP

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Permissão de acesso à raiz"](#).

Sobre esta tarefa

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

Todos os nós na grade usam a mesma configuração SNMP.

Especifique a configuração básica

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

Passos

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

A página do agente SNMP é exibida.

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

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

Campo	Descrição
Localização do sistema	<p>Opcional. A localização do sistema StorageGRID, que é retornado em mensagens SNMP como sysLocation.</p> <p>A localização do sistema pode ser qualquer informação útil para identificar onde o sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. Esse valor se aplica a todos os nós no sistema StorageGRID. A localização do sistema pode ter no máximo 255 caracteres.</p>
Ativar notificações de agente SNMP	<ul style="list-style-type: none"> • Se selecionado, o agente SNMP do StorageGRID envia trap e informa notificações. • Se não estiver selecionado, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.
Ativar traps de autenticação	Se selecionado, o agente SNMP do StorageGRID envia traps de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Introduza cadeias de caracteres da comunidade

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

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

Passos

1. Para **comunidade somente leitura**, opcionalmente, insira uma cadeia de caracteres comunitária para permitir acesso MIB somente leitura em endereços de agentes IPv4 e IPv6.



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

Cada string 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.

Até cinco cordas são permitidas.

Crie destinos de armadilha

Use a guia Trap Destinations (destinos de intercetção) na seção Other configurations (outras configurações) para definir um ou mais destinos para o StorageGRID trap (trap de intercetção) ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

Passos

1. Para o campo **Default trap Community** (comunidade de trap padrão), insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de trap SNMPv1 ou SNMPv2.

Conforme necessário, você pode fornecer uma string de comunidade ("personalizada") diferente quando você define um destino de armadilha específico.

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

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

SNMPv1

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

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

SNMPv2c

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

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

SNMPv3

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

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de intercetção SNMP, a menos que você precise usar TCP.
Utilizador USM	<p>O utilizador USM que será utilizado para autenticação.</p> <ul style="list-style-type: none"> • Se selecionou Trap, apenas são apresentados utilizadores USM sem IDs de motor autoritativas. • Se selecionou inform, apenas são apresentados utilizadores USM com IDs de motor autoritativas. • Se não forem apresentados utilizadores: <ul style="list-style-type: none"> i. Crie e salve o destino da armadilha. ii. Vá para Crie utilizadores USM e crie o usuário. iii. Regresse ao separador Trap Destinations (destinos da armadilha), selecione o destino guardado na tabela e selecione Edit (Editar). iv. Selecione o utilizador.

5. Selecione **criar**.

O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agente

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

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

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Protocolo da Internet	Se esse endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se esse endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Qual rede StorageGRID o agente ouvirá. <ul style="list-style-type: none"> • Redes Grid, Admin e Client: O agente SNMP escutará consultas em todas as três redes. • Rede de rede • Rede de administração • Rede de clientes <p>Nota: Se você usar a rede do cliente para dados inseguros e criar um endereço de agente para a rede do cliente, esteja ciente de que o tráfego SNMP também será inseguro.</p>
Porta	Opcionalmente, o número da porta que o agente SNMP deve ouvir. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. Nota: Quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

3. Selecione **criar**.

O endereço do agente é criado e adicionado à tabela.

Crie utilizadores USM

Se estiver a utilizar o SNMPv3, utilize o separador utilizadores USM na secção outras configurações para definir os utilizadores USM que estão autorizados a consultar o MIB ou a receber traps e informações.



SNMPv3 *inform* destinos devem ter usuários com IDs de motor. SNMPv3 *trap* destino não pode ter usuários com IDs de motor.

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

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Nome de utilizador	Um nome exclusivo para este utilizador USM. Os nomes de usuário podem ter um máximo de 32 caracteres e não podem conter caracteres de espaço em branco. O nome de usuário não pode ser alterado depois que o usuário é criado.
Acesso MIB somente leitura	Se selecionado, este utilizador deverá ter acesso apenas de leitura à MIB.
ID do motor autoritário	Se este utilizador for utilizado num destino de informação, o ID de mecanismo autorizado para este utilizador. Insira 10 a 64 caracteres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para utilizadores USM que serão selecionados em destinos de armadilha para informação. Este valor não é permitido para utilizadores USM que serão selecionados em destinos de armadilha para armadilhas. Nota: Este campo não é mostrado se você selecionou Acesso MIB somente leitura porque os usuários USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o utilizador USM: <ul style="list-style-type: none"> • AuthPriv: Este usuário se comunica com autenticação e privacidade (criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe, um protocolo de privacidade e uma palavra-passe. • AuthNoPriv: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Palavra-passe	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Mostrado apenas se você selecionou authPriv e sempre definido como AES, que é o único protocolo de privacidade suportado.
Palavra-passe	Mostrado apenas se você selecionou authPriv . A senha que este usuário usará para privacidade.

3. Selecione **criar**.

O utilizador USM é criado e adicionado à tabela.

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

A nova configuração do agente SNMP fica ativa.

Atualize o agente SNMP

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Permissão de acesso à raiz"](#).

Sobre esta tarefa

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

Passos

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

A página do agente SNMP é exibida.

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

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

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

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

- c. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar traps de autenticação** para controlar se o agente SNMP do StorageGRID envia traps de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usar SNMPv1 ou SNMPv2c, opcionalmente, atualize ou adicione uma comunidade **somente leitura** na seção cadeias de Comunidade.
 5. Para atualizar destinos de intercetação, selecione a guia destinos de intercetação na seção outras configurações.

Utilize este separador para definir um ou mais destinos para o StorageGRID trap ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

Para obter detalhes sobre o que introduzir, ["Criar destinos de armadilha"](#) consulte .

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

Se você remover a comunidade de trap padrão, primeiro deve garantir que todos os destinos de trap

existentes usem uma cadeia de caracteres de comunidade personalizada.

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

6. Para atualizar endereços de agentes, selecione a guia endereços de agentes na seção outras configurações.

Use esta guia para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Para obter detalhes sobre o que introduzir, "[Criar endereços de agente](#)" consulte .

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

7. Para atualizar os utilizadores USM, selecione o separador utilizadores USM na seção outras configurações.

Utilize este separador para definir os utilizadores USM que estão autorizados a consultar a MIB ou a receber traps e informações.

Para obter detalhes sobre o que introduzir, "[Crie utilizadores USM](#)" consulte .

- Para adicionar um utilizador USM, selecione **criar**.
- Para editar um utilizador USM, selecione o botão de opção e selecione **Edit**.

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



Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, você deverá editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

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



Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deve editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

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

8. Quando tiver atualizado a configuração do agente SNMP, selecione **Save**.

Acesse arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e

serviços gerenciados para os nós em sua grade. Você pode acessar arquivos MIB que definem os objetos e notificações do StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Consulte ["Utilize a monitorização SNMP"](#) para obter mais informações sobre ficheiros SNMP e MIB.

Acesse arquivos MIB

Siga estes passos para aceder aos ficheiros MIB.

Passos

1. Selecione **CONFIGURATION > Monitoring > SNMP Agent**.
2. Na página do agente SNMP, selecione o arquivo que deseja baixar:
 - **NetApp-StorageGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os nós de administração.
 - *** ES-NetApp-06-MIB.mib***: Define objetos e notificações para dispositivos baseados em série e.
 - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com interface BMC.



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

3. Para extrair os OIDs StorageGRID do arquivo MIB:

- a. Obtenha o OID da raiz do MIB do StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Resultado: `.1.3.6.1.4.1.789.28669` (28669 É sempre o OID para StorageGRID)

- a. Grep para o OID StorageGRID em toda a árvore (usando `paste` para unir linhas):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



O `snmptranslate` comando tem muitas opções que são úteis para explorar o MIB. Este comando está disponível em qualquer nó StorageGRID.

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID StorageGRID.

Nome do objeto	Código Objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID.

Objetos MIB

Nome do objeto	Código Objeto (OID)	Descrição
ActiveAlertCount		O número de alertas ativos na activeAlertTable.
ActiveAlertTable		Uma tabela de alertas ativos no StorageGRID.
ActiveAlertId		O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
ActiveAlertName		O nome do alerta.
ActiveAlertInstance		O nome da entidade que gerou o alerta, normalmente o nome do nó.
ActiveAlertSeverity		A gravidade do alerta.
ActiveAlertStartTime		A data e a hora em que o alerta foi acionado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo de notificação	Código Objeto (OID)	Descrição
ActiveMinorAlert		Um alerta com gravidade menor
ActiveMajorAlert		Um alerta com grande gravidade
ActiveCriticalAlert		Um alerta com gravidade crítica

Colete dados adicionais do StorageGRID

Use gráficos e relatórios

Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas.

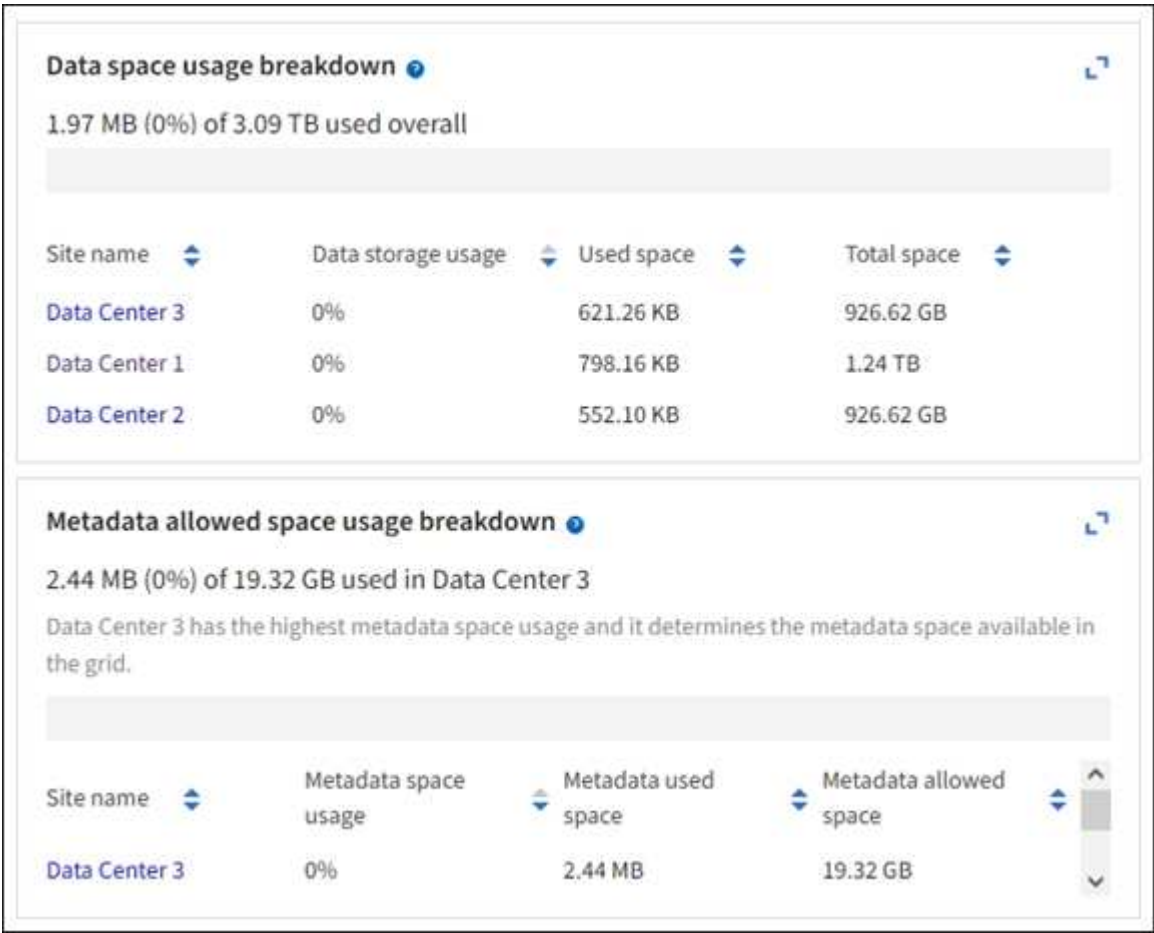


O Gerenciador de Grade é atualizado com cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

Tipos de gráficos

Gráficos e gráficos resumem os valores de métricas e atributos específicos do StorageGRID.

O painel do Gerenciador de Grade inclui cartões que resumem o armazenamento disponível para a grade e cada local.



O painel uso do armazenamento no painel do Gerenciador do locatário exibe o seguinte:

- Uma lista dos maiores baldes (S3) ou contentores (Swift) para o inquilino
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou contentores
- A quantidade total de espaço utilizado e, se for definida uma quota, a quantidade e a percentagem de espaço restante

Dashboard

16

Buckets

[View buckets](#)

2

Platform services

endpoints
[View endpoints](#)

0

Groups

[View groups](#)

1

User

[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details [?](#)

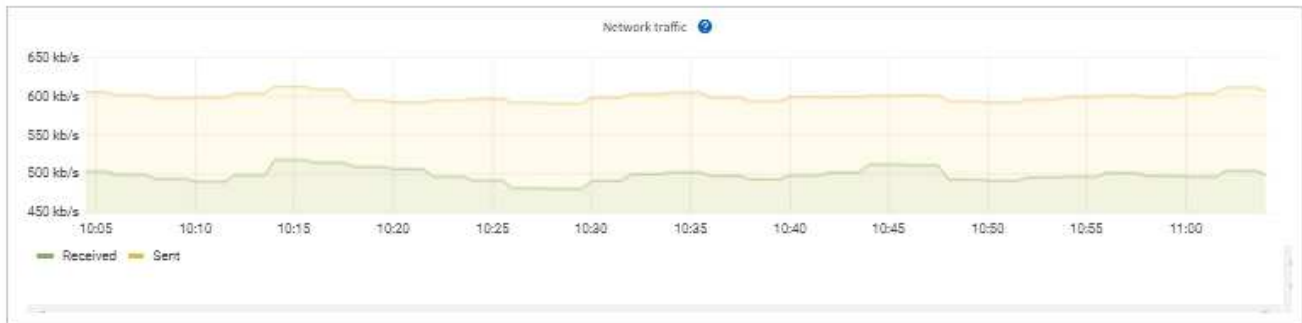
Name: Tenant02
ID: 3341 1240 0546 8283 2208
✓ Platform services enabled
✓ Can use own identity source
✓ S3 Select enabled

Além disso, gráficos que mostram como as métricas e atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página de nós e na página **SUPPORT > Tools > Grid topology**.

Existem quatro tipos de gráficos:

- **Gráficos Grafana:** Mostrados na página de nós, gráficos Grafana são usados para plotar os valores das métricas Prometheus ao longo do tempo. Por exemplo, a guia **NÓS > rede** para um nó de armazenamento inclui um gráfico Grafana para tráfego de rede.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

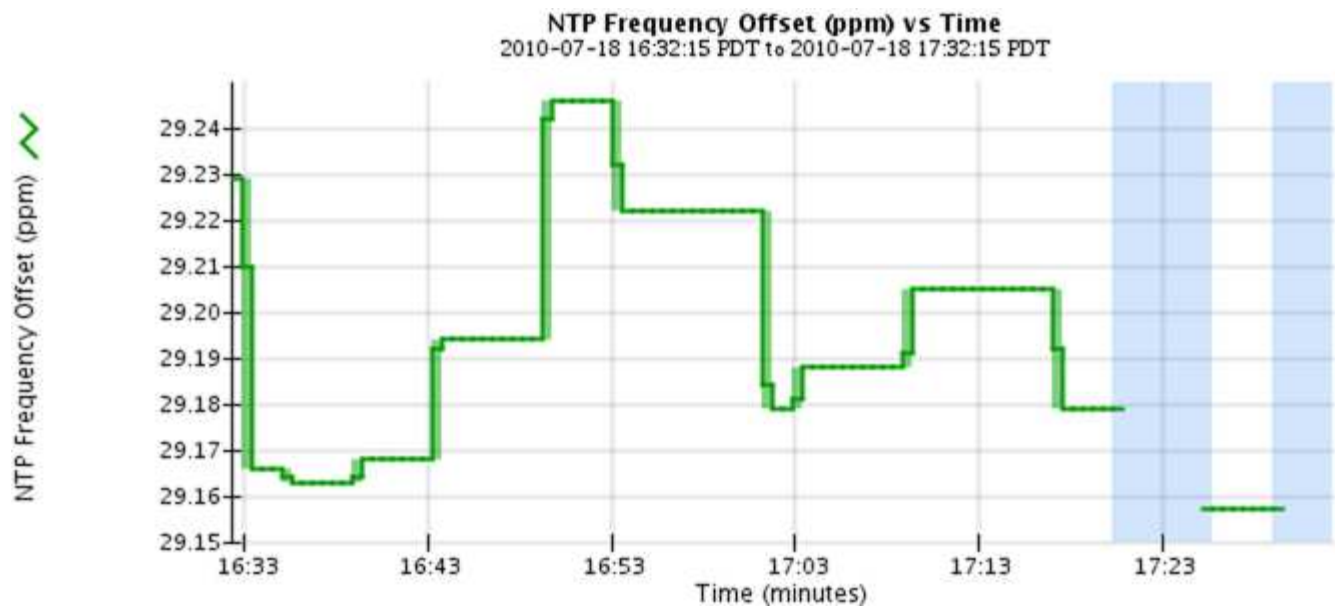
Transmit


Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

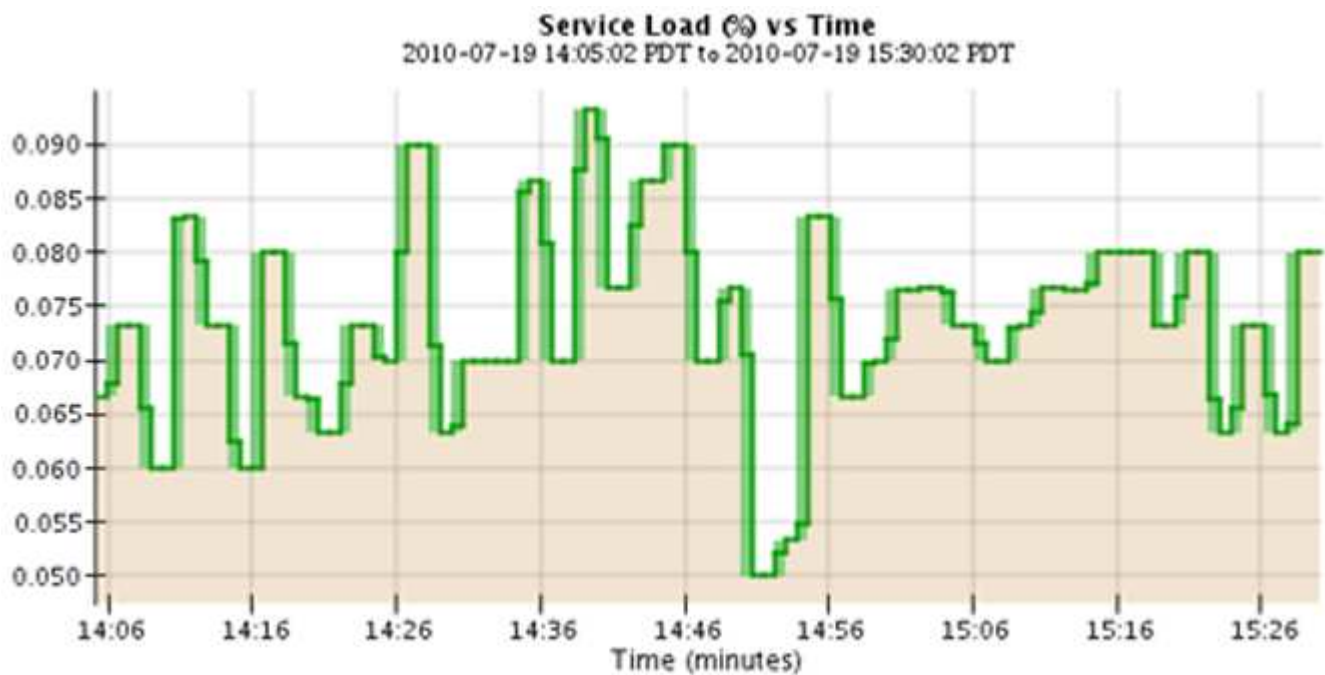


Gráficos Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPPORT > Tools > Metrics**.

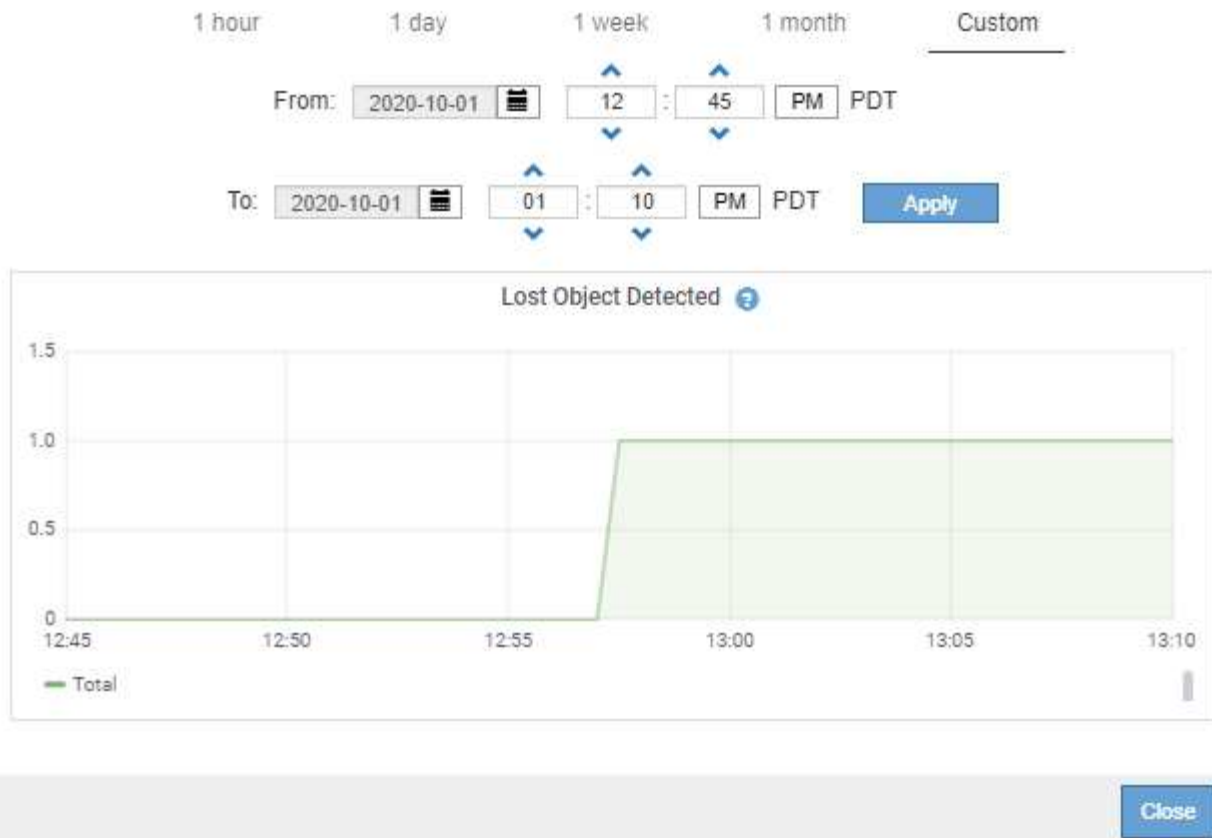
- **Gráficos de linha:** Disponíveis na página de nós e na página **SUPPORT > Tools > Grid topology** (selecione o ícone do gráfico após um valor de dados), os gráficos de linha são usados para plotar os valores dos atributos StorageGRID que têm um valor unitário (como deslocamento de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.




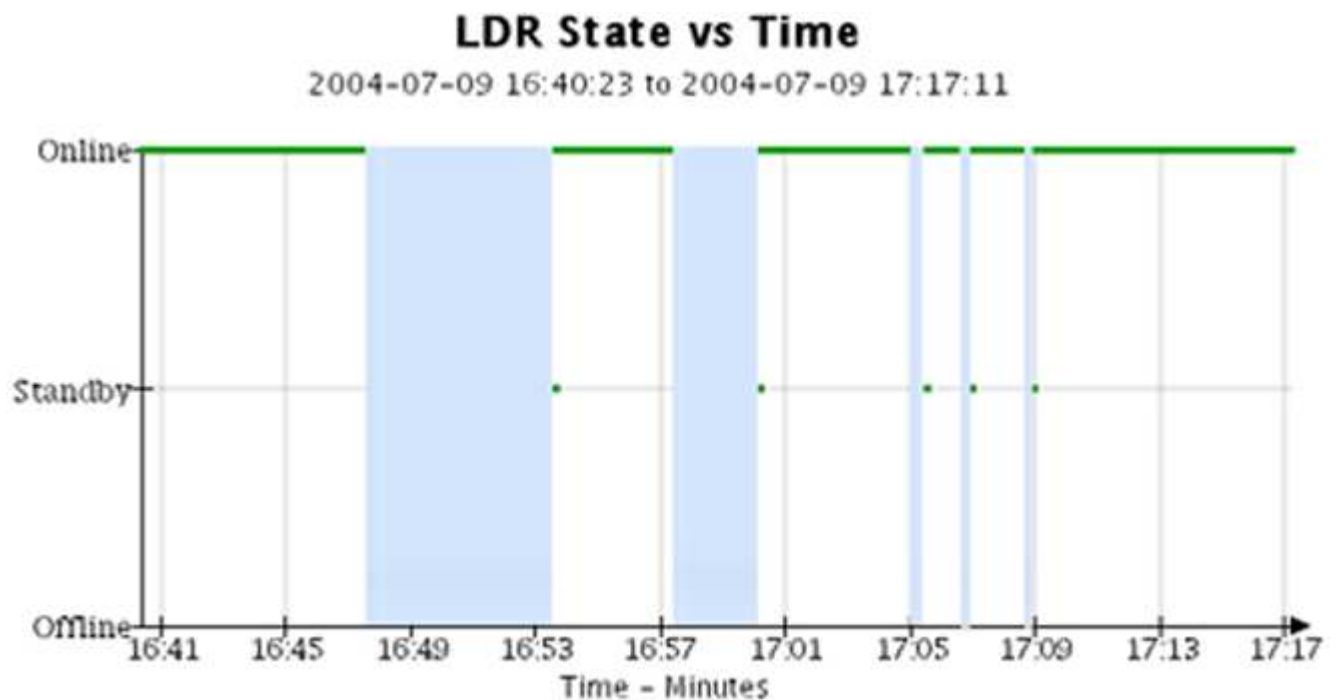
- **Gráficos de área:** Disponíveis na página de nós e na página **SUPPORT > Tools > Grid topology** (selecione o ícone do gráfico  após um valor de dados), os gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. Os gráficos de área são semelhantes aos gráficos de linha, mas incluem um sombreamento marrom claro abaixo da linha. As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



- Alguns gráficos são denotados com um tipo diferente de ícone de gráfico  e têm um formato diferente:



- **State graph:** Disponível na página **SUPPORT > Tools > Grid topology** (selecione o ícone do gráfico  após um valor de dados), os gráficos de estado são usados para plotar valores de atributo que representam estados distintos, como um estado de serviço que pode ser on-line, standby ou offline. Os gráficos de estado são semelhantes aos gráficos de linha, mas a transição é descontínua, ou seja, o valor salta de um valor de estado para outro.



Informações relacionadas







["Exibir a página nós"](#)

["Veja a árvore de topologia de Grade"](#)

["Analise as métricas de suporte"](#)

Legenda da carta

As linhas e cores usadas para desenhar gráficos têm significado específico.

Exemplo	Significado
	Os valores de atributo relatados são plotados usando linhas verdes escuras.
	O sombreamento verde claro em torno de linhas verdes escuras indica que os valores reais nesse intervalo de tempo variam e foram "encadernados" para plotagem mais rápida. A linha escura representa a média ponderada. O intervalo em verde claro indica os valores máximo e mínimo dentro do compartimento. O sombreamento castanho claro é usado para gráficos de área para indicar dados volumétricos.
	Áreas em branco (sem dados plotados) indicam que os valores do atributo não estavam disponíveis. O fundo pode ser azul, cinza ou uma mistura de cinza e azul, dependendo do estado do serviço que relata o atributo.
	O sombreamento azul claro indica que alguns ou todos os valores do atributo naquele momento eram indeterminados; o atributo não estava relatando valores porque o serviço estava em um estado desconhecido.
	O sombreamento cinza indica que alguns ou todos os valores de atributo naquele momento não eram conhecidos porque o serviço que relata os atributos estava administrativamente inativo.
	Uma mistura de sombreamento cinza e azul indica que alguns dos valores de atributo na época eram indeterminados (porque o serviço estava em um estado desconhecido), enquanto outros não eram conhecidos porque o serviço relatando os atributos estava administrativamente para baixo.

Apresentar gráficos e gráficos

A página nós contém os gráficos e gráficos que você deve acessar regularmente para monitorar atributos como capacidade de storage e taxa de transferência. Em alguns casos, especialmente ao trabalhar com suporte técnico, você pode usar a página **SUPPORT > Tools > Grid topology** para acessar gráficos adicionais.

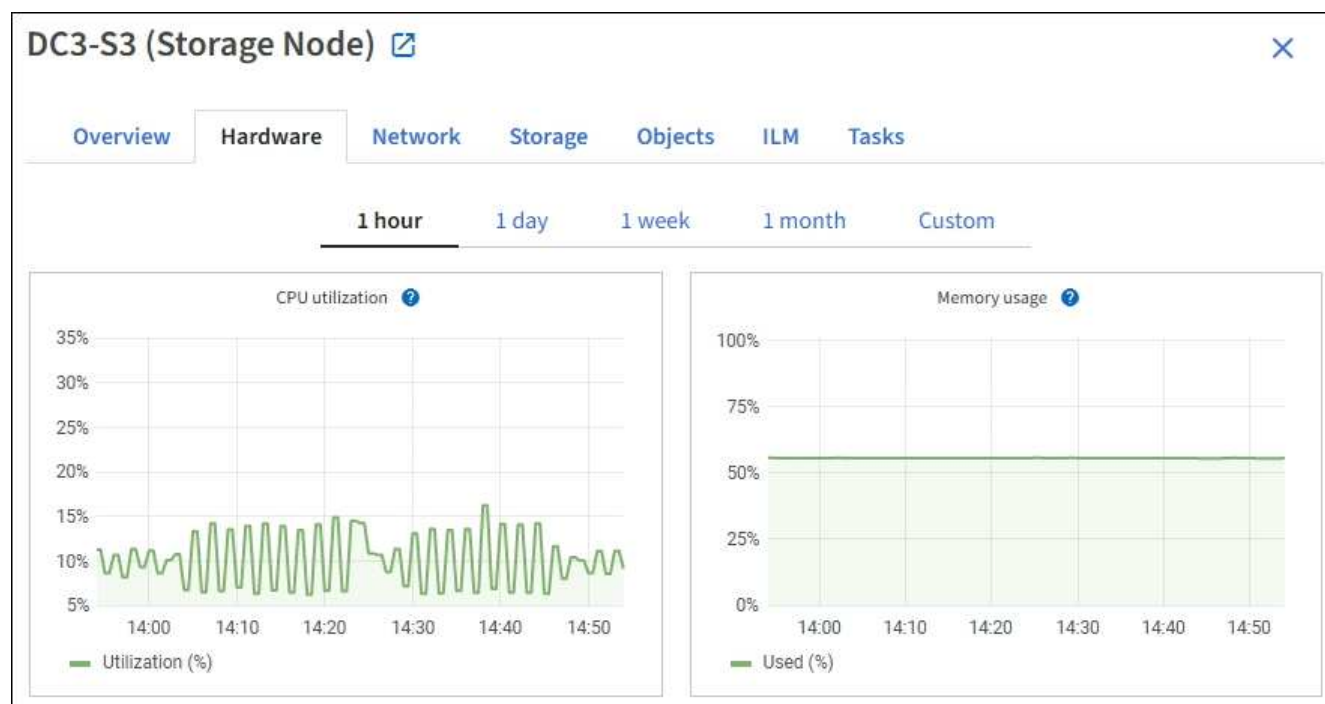
Antes de começar

Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).

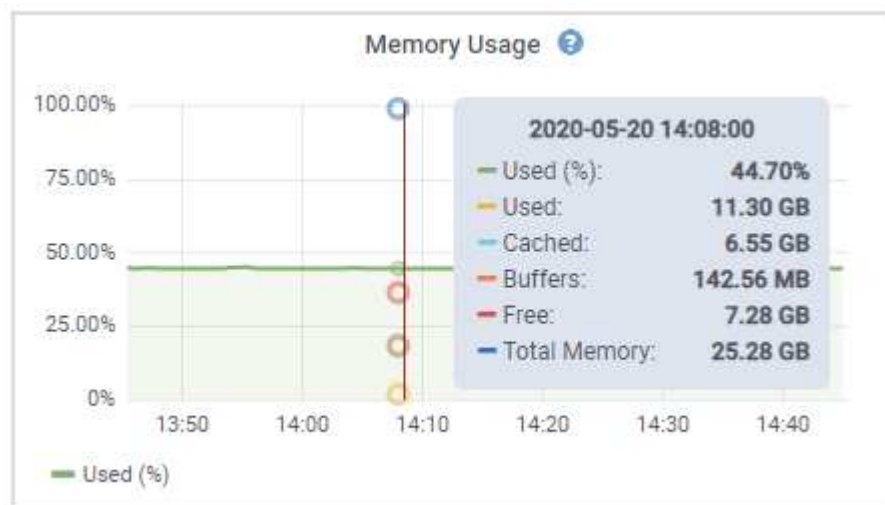
Passos

1. Selecione **NODES**. Em seguida, selecione um nó, um site ou toda a grade.
2. Selecione o separador para o qual pretende ver as informações.

Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas de Prometheus ao longo do tempo. Por exemplo, a guia **NÓS > hardware** de um nó inclui dois gráficos Grafana.



3. Opcionalmente, posicione o cursor sobre o gráfico para ver valores mais detalhados para um determinado ponto no tempo.



4. Conforme necessário, muitas vezes é possível exibir um gráfico para um atributo ou métrica específico. Na tabela na página nós, selecione o ícone do gráfico à direita do nome do atributo.



Os gráficos não estão disponíveis para todas as métricas e atributos.

Exemplo 1: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o número total de consultas de armazenamento de metadados bem-sucedidas para o nó de armazenamento.



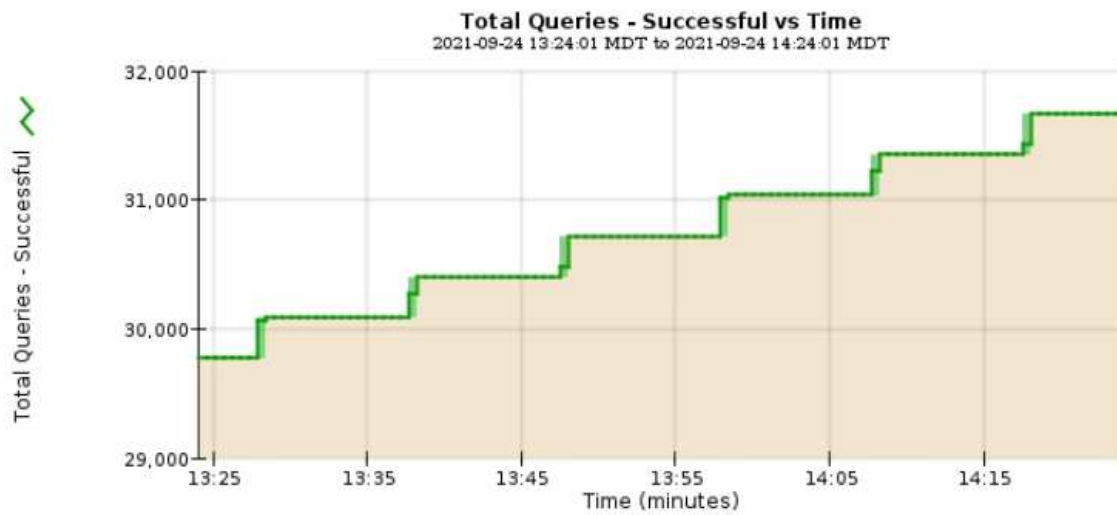
Reports (Charts): DDS (DC1-S1) - Data Store



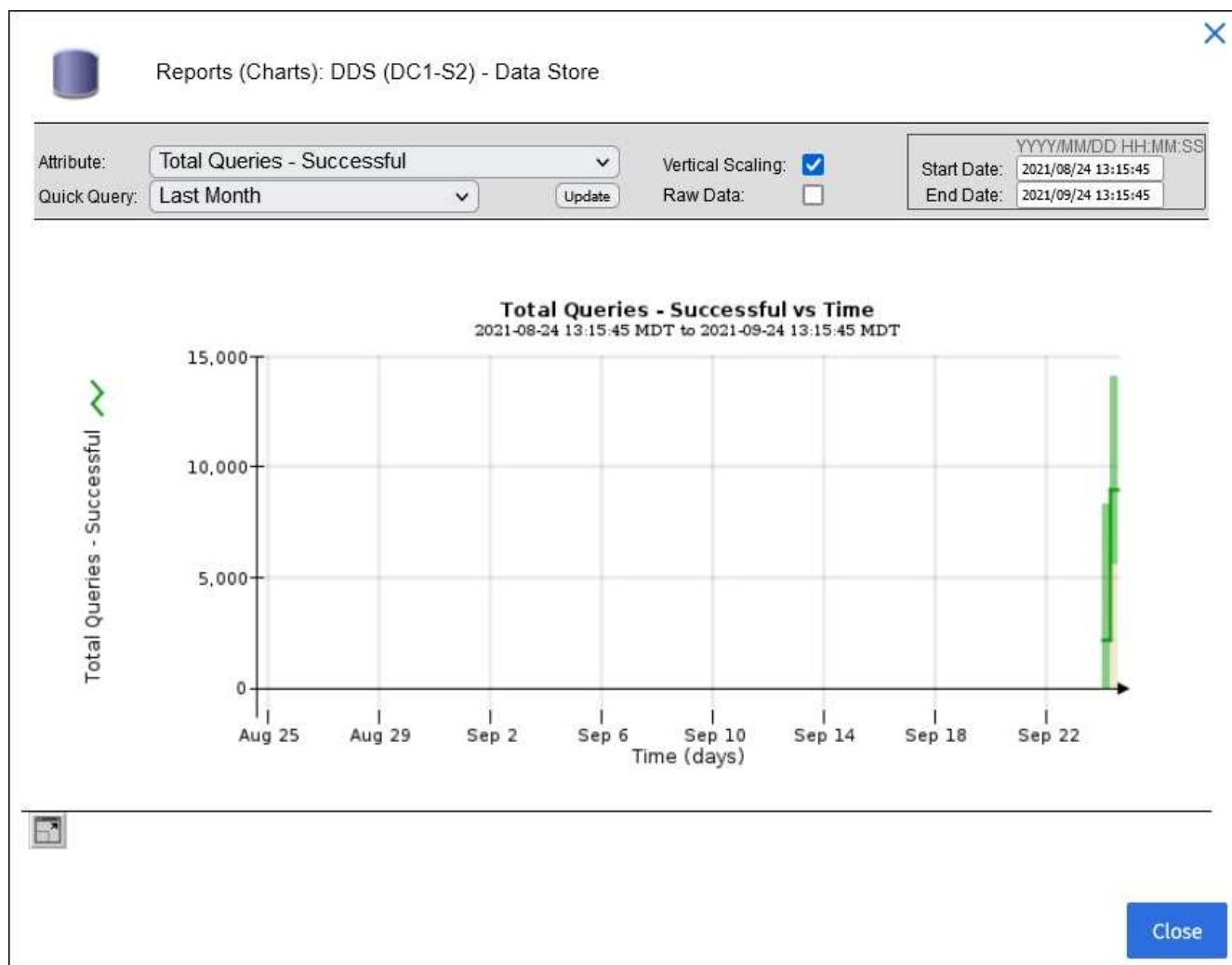
Attribute: Total Queries - Successful
Quick Query: Last Hour Update


Vertical Scaling: ☒
Raw Data: ☐

YYYY/MM/DD HH:MM:SS
Start Date: 2021/09/24 13:24:01
End Date: 2021/09/24 14:24:01




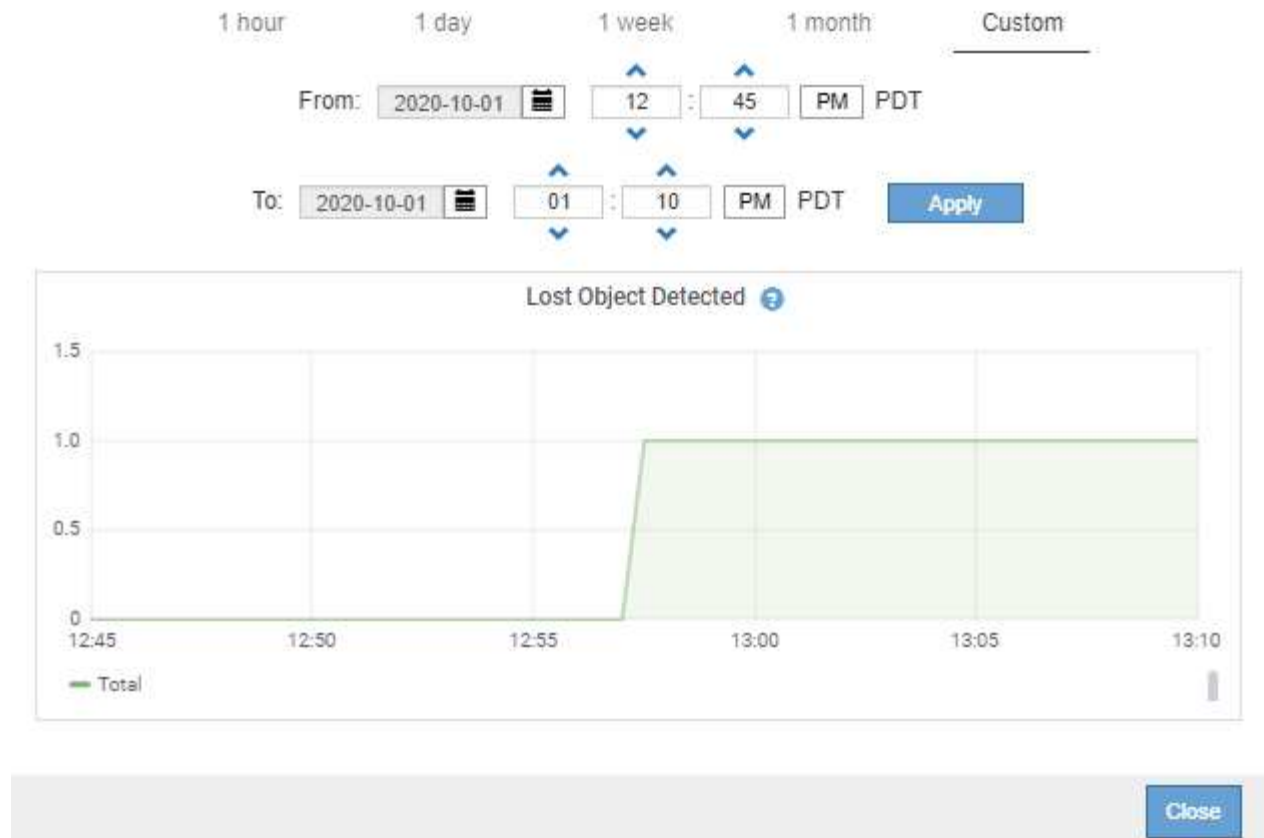
Close



Exemplo 2: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico  para ver o gráfico Grafana da contagem de objetos perdidos detetados ao longo do tempo.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Para exibir gráficos para atributos que não são exibidos na página nó, selecione **support > Tools > Grid topology**.
6. Selecione **grid node > component ou Service > Overview > Main**.

Overview

Alarms

Reports

Configuration



Main



Overview: SSM (DC1-ADM1) - Resources

Updated: 2018-05-07 16:29:52 MDT

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Selecione o ícone do gráfico  ao lado do atributo.

O visor muda automaticamente para a página **relatórios > gráficos**. O gráfico exibe os dados do atributo no último dia.

Gerar gráficos

Os gráficos exibem uma representação gráfica dos valores de dados de atributos. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#)tem .

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **grid node > component ou Service > Reports > Charts**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Para forçar o eixo Y a iniciar em zero, desmarque a caixa de seleção **vertical Scaling**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **dados brutos** ou arredondar valores

para um máximo de três casas decimais (por exemplo, para atributos reportados como porcentagens), desmarque a caixa de seleção **dados brutos**.

6. Selecione o período de tempo para relatar na lista suspensa **consulta rápida**.

Selecione a opção consulta personalizada para selecionar um intervalo de tempo específico.

O gráfico aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

7. Se você selecionou consulta personalizada, personalize o período de tempo para o gráfico inserindo **Data de início** e **Data de término**.

Utilize o formato `YYYY/MM/DDHH:MM:SS` na hora local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Selecione **Atualizar**.

Um gráfico é gerado após alguns segundos. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.

Use relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Existem dois tipos de relatórios gerados dependendo do período de tempo em que você está relatando: Relatórios de texto bruto para períodos inferiores a uma semana e relatórios de texto agregados para períodos de tempo superiores a uma semana.

Relatórios de texto bruto

Um relatório de texto bruto exibe detalhes sobre o atributo selecionado:

- Hora recebida: Data e hora local em que um valor de amostra dos dados de um atributo foi processado pelo serviço NMS.
- Hora da amostra: Data e hora locais em que um valor de atributo foi amostrado ou alterado na origem.
- Valor: Valor do atributo no tempo da amostra.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Agregar relatórios de texto

Um relatório de texto agregado exibe dados durante um período de tempo mais longo (geralmente uma semana) do que um relatório de texto bruto. Cada entrada é o resultado de resumir vários valores de atributo (um agregado de valores de atributo) pelo serviço NMS ao longo do tempo em uma única entrada com valores médios, máximos e mínimos que são derivados da agregação.

Cada entrada exibe as seguintes informações:

- Hora agregada: Data e hora locais da última vez que o serviço NMS agregou (coletou) um conjunto de valores de atributo alterados.
- Valor médio: A média do valor do atributo durante o período de tempo agregado.
- Valor mínimo: O valor mínimo durante o período de tempo agregado.
- Valor máximo: O valor máximo durante o período de tempo agregado.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Gerar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Você pode gerar relatórios em um local de data center, nó de grade, componente ou serviço.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#) tem .

Sobre esta tarefa

Para dados de atributos que se espera que estejam mudando continuamente, esses dados de atributo são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributos que mudam com pouca frequência (por exemplo, dados baseados em eventos como alterações de estado ou status), um valor de atributo é enviado ao serviço NMS quando o valor muda.

O tipo de relatório apresentado depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos de tempo superiores a uma semana.

Texto cinza indica que o serviço foi desativado administrativamente durante o período de amostragem. Texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **grid node > component ou Service > Reports > Text**.
3. Selecione o atributo para relatar na lista suspensa **Atributo**.
4. Selecione o número de resultados por página na lista suspensa **resultados por página**.
5. Para arredondar valores para um máximo de três casas decimais (por exemplo, para atributos reportados como porcentagens), desmarque a caixa de seleção **dados brutos**.
6. Selecione o período de tempo para relatar na lista suspensa **consulta rápida**.

Selecione a opção consulta personalizada para selecionar um intervalo de tempo específico.

O relatório aparece após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo.

- Se você selecionou consulta personalizada, você precisa personalizar o período de tempo para relatar inserindo **Data de início** e **Data de término**.

Utilize o formato YYYY/MM/DDHH:MM:SS na hora local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

- Clique em **Atualizar**.

Um relatório de texto é gerado após alguns momentos. Aguarde vários minutos para a tabulação de longos intervalos de tempo. Dependendo do período de tempo definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado são exibidos.


Exportar relatórios de texto

Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

Sobre esta tarefa


Os dados copiados podem então ser salvos em um novo documento (por exemplo, uma Planilha) e usados para analisar o desempenho do sistema StorageGRID.

Passos

- Selecione **SUPPORT > Tools > Grid topology**.
- Crie um relatório de texto.
- Clique em ***Exportar*** .

OverviewAlarmsReportsConfiguration

ChartsText

**Reports (Text): SSM (170-176) - Events**

Attribute:Attribute Send to Relay Rate

Quick Query:Custom Query

Update

Results Per Page:5


Raw Data:☒

YYYY/MM/DD HH:MM:SS

Start Date:2010/07/19 08:42:09

End Date:2010/07/20 08:42:09

Text Results for Attribute Send to Relay Rate
2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254 

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

A janela Exportar relatório de texto abre-se exibindo o relatório.

Grid ID: 000 000
 OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
 Node Path: Site/170-176/SSM/Events
 Attribute: Attribute Send to Relay Rate (ABSR)
 Query Start Date: 2010-07-19 08:42:09 PDT
 Query End Date: 2010-07-20 08:42:09 PDT
 Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
 2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
 2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
 2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
 2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
 2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
 2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
 2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
 2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
 2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
 2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
 2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
 2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
 2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Selecione e copie o conteúdo da janela Exportar Relatório de texto.

Esses dados podem agora ser colados em um documento de terceiros, como uma Planilha.

Monitore O PUT e obtenha desempenho

Você pode monitorar o desempenho de certas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir mais investigação.

Sobre esta tarefa

Para monitorar O desempenho, você pode executar comandos S3 e Swift diretamente de uma estação de trabalho ou usando o aplicativo S3tester de código aberto. O uso desses métodos permite avaliar o desempenho independentemente de fatores externos ao StorageGRID, como problemas com um aplicativo cliente ou problemas com uma rede externa.

Ao executar testes de OPERAÇÕES put and GET, use as seguintes diretrizes:

- Use tamanhos de objeto comparáveis aos objetos que você normalmente ingere em sua grade.
- Realize operações em locais locais e remotos.

As mensagens na "[log de auditoria](#)" indicam o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação GET S3, você pode revisar o valor do ATRIBUTO TIME na mensagem de auditoria SGET. Você também pode encontrar o ATRIBUTO TIME nas mensagens de auditoria para as seguintes operações:

- **S3:** EXCLUIR, OBTER, CABEÇA, METADADOS ATUALIZADOS, POSTAR, COLOCAR
- **SWIFT:** EXCLUIR, OBTER, CABEÇA, COLOCAR

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o throughput geral que você pode alcançar. Repita os mesmos testes regularmente e registre os resultados, para

que possa identificar tendências que possam necessitar de investigação.

- Você pode ["Baixe S3tester a partir de github"](#).

Monitorar operações de verificação de objetos

O sistema StorageGRID pode verificar a integridade dos dados de objetos nos nós de storage, verificando se há objetos corrompidos ou ausentes.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Permissão de manutenção ou acesso root"](#).

Sobre esta tarefa

Dois ["processos de verificação"](#) trabalham juntos para garantir a integridade dos dados:

- * A verificação em segundo plano* é executada automaticamente, verificando continuamente a correção dos dados do objeto.

A verificação em segundo plano verifica automaticamente e continuamente todos os nós de storage para determinar se há cópias corrompidas de dados de objetos replicados e codificados por apagamento. Se forem encontrados problemas, o sistema StorageGRID tentará substituir automaticamente os dados de objetos corrompidos de cópias armazenadas em outro lugar do sistema. A verificação em segundo plano não é executada em nós de arquivamento ou em objetos em um pool de storage de nuvem.



O alerta **Objeto corrompido não identificado detetado** é acionado se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente.

- **A verificação de existência de objetos** pode ser acionada por um usuário para verificar mais rapidamente a existência (embora não a correção) de dados de objetos.

A verificação de existência de objeto verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados por apagamento existem em um nó de storage. A verificação de existência de objeto fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware poderia ter afetado a integridade dos dados.

Você deve rever os resultados de verificações de antecedentes e verificações de existência de objetos regularmente. Investigue quaisquer instâncias de dados de objetos corrompidos ou ausentes imediatamente para determinar a causa raiz.

Passos

1. Reveja os resultados das verificações de antecedentes:
 - a. Selecione **NODES > Storage Node > Objects**.
 - b. Verifique os resultados da verificação:
 - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- Para verificar a verificação de fragmentos codificados por apagamento, selecione **Storage Node > ILM** e veja os atributos na seção de verificação de codificação de apagamento.

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Selecione o ponto de interrogação ? ao lado do nome de um atributo para exibir o texto da ajuda.

2. Reveja os resultados dos trabalhos de verificação de existência de objeto:

a. Selecione **MAINTENANCE > Object existence check > Job history**.

b. Digitalizar a coluna cópias de objeto em falta detetadas. Se algum trabalho resultar em 100 ou mais cópias de objetos ausentes e o alerta **objetos perdidos** tiver sido acionado, entre em Contato com o suporte técnico.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job

Job history

Delete

Search...

☐

Job ID ?

Status ?

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

0

Monitorar eventos

Você pode monitorar eventos que são detetados por um nó de grade, incluindo eventos personalizados que você criou para rastrear eventos registrados no servidor syslog. A mensagem último evento mostrada no Gerenciador de Grade fornece mais informações sobre o evento mais recente.

As mensagens de evento também são listadas no `/var/local/log/bycast-err.log` arquivo de log. Consulte "[Referência de arquivos de registro](#)".

O alarme SMTT (Total de eventos) pode ser repetidamente acionado por problemas como problemas de rede, interrupções de energia ou atualizações. Esta seção tem informações sobre a investigação de eventos para que você possa entender melhor por que esses alarmes ocorreram. Se um evento ocorreu devido a um problema conhecido, é seguro redefinir os contadores de eventos.

Passos

- Revise os eventos do sistema para cada nó de grade:
 - Selecione **SUPPORT > Tools > Grid topology**.
 - Selecione **site > grid node > SSM > Eventos > Visão geral > Principal**.
- Gere uma lista de mensagens de eventos anteriores para ajudar a isolar problemas que ocorreram no passado:

- Selecione **SUPPORT > Tools > Grid topology**.
- Selecione **site > grid node > SSM > Eventos > relatórios**.
- Selecione **texto**.

O atributo **último evento** não é mostrado no "vista de gráficos". Para visualizá-lo:

- Altere **Atributo** para **último evento**.
- Opcionalmente, selecione um período de tempo para **consulta rápida**.
- Selecione **Atualizar**.

Reports (Text): SSM (170-41) - Events

Attribute: Last Event Results Per Page: 20 Start Date: 2009/04/15 15:19:53
 Quick Query: Last 5 Minutes Update Raw Data: ☒ End Date: 2009/04/15 15:24:53

Text Results for Last Event
 2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Crie eventos syslog personalizados

Eventos personalizados permitem que você acompanhe todos os eventos de usuário do kernel, daemon, erro e nível crítico registrados no servidor syslog. Um evento personalizado pode ser útil para monitorar a ocorrência de mensagens de log do sistema (e, portanto, eventos de segurança de rede e falhas de hardware).

Sobre esta tarefa



Considere criar eventos personalizados para monitorar problemas recorrentes. As considerações a seguir se aplicam a eventos personalizados.


- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada.
- Para criar um evento personalizado com base em palavras-chave nos `/var/local/log/messages` arquivos, os logs nesses arquivos devem ser:
 - Gerado pelo kernel
 - Gerado pelo daemon ou programa do usuário no nível de erro ou crítico

Nota: nem todas as entradas nos `/var/local/log/messages` arquivos serão correspondidas a menos que satisfaçam os requisitos acima indicados.

Passos



- Selecione **SUPPORT > Alarmes (legacy) > Custom events**.

2. Clique em **Edit**  (ou **Insert**  se este não for o primeiro evento).
3. Introduza uma cadeia de eventos personalizada, por exemplo, encerramento




Events
 Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1) 

Event	Actions
shutdown	   

Show Records Per Page

 Previous « 1 » Next




4. Selecione **aplicar alterações**.
5. Selecione **SUPPORT > Tools > Grid topology**.
6. Selecione **grid node > SSM > Eventos**.
7. Localize a entrada de Eventos personalizados na tabela Eventos e monitore o valor de **Count**.

Se a contagem aumentar, um evento personalizado que você está monitorando está sendo acionado nesse nó de grade.

Overview
Alarms
Reports
Configuration

Main



Overview: SSM (DC1-ADM1) - Events
Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State: Connected
Total Events: 0
Last Event: No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

Redefina a contagem de eventos personalizados para zero

Se você quiser redefinir o contador apenas para eventos personalizados, use a página topologia de grade no menu suporte.

A reposição de um contador faz com que o alarme seja acionado pelo próximo evento. Em contraste, quando você reconhece um alarme, esse alarme só é reacionado se o próximo nível de limiar for atingido.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **grid node > SSM > Eventos > Configuração > Principal**.
3. Marque a caixa de seleção **Reset** para Eventos personalizados.

Overview


Alarms

Reports

Configuration

Main

Alarms



Configuration: SSM (DC2-ADM1) - Events

Updated: 2018-04-11 10:35:44 MDT

Description	Count	Reset
Abnormal Software Events	0	<input type="checkbox"/>
Account Service Events	0	<input type="checkbox"/>
Cassandra Errors	0	<input type="checkbox"/>
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>
Custom Events	0	<input checked="" type="checkbox"/>
File System Errors	0	<input type="checkbox"/>
Forced Termination Events	0	<input type="checkbox"/>

4. Selecione **aplicar alterações**.

Rever mensagens de auditoria

As mensagens de auditoria podem ajudá-lo a entender melhor as operações detalhadas do seu sistema StorageGRID. Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços StorageGRID geram mensagens de auditoria, como segue:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de storage de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento Registram solicitações de usuários para a API de gerenciamento.

Cada nó Admin armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compactados de dias anteriores. Cada nó na grade também armazena uma cópia das informações de auditoria geradas no nó.

Para facilitar o acesso aos logs de auditoria, você pode ["Configurar acesso de cliente de auditoria para NFS"](#). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

O StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- O padrão do StorageGRID é destinos de auditoria de nó local.

- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de storage.
- Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado.
- ["Saiba mais sobre como configurar mensagens de auditoria e destinos de log"](#).

Para obter detalhes sobre o arquivo de log de auditoria, o formato das mensagens de auditoria, os tipos de mensagens de auditoria e as ferramentas disponíveis para analisar mensagens de auditoria, ["Rever registros de auditoria"](#) consulte .

Colete arquivos de log e dados do sistema

Você pode usar o Gerenciador de Grade para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade no nó Admin principal usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#)tem .
- Você deve ter a senha de provisionamento.

Sobre esta tarefa

Você pode usar o Gerenciador de Grade para coletar ["ficheiros de registo"](#), dados do sistema e dados de configuração de qualquer nó de grade para o período de tempo selecionado. Os dados são coletados e arquivados em um arquivo .tar.gz que você pode baixar para seu computador local.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado. ["Configurar mensagens de auditoria e destinos de log"](#)Consulte .

Passos

1. Selecione **SUPPORT > Tools > Logs**.

2. Selecione os nós de grade para os quais você deseja coletar arquivos de log.

Conforme necessário, você pode coletar arquivos de log para toda a grade ou para todo o site do data center.

3. Selecione **hora de início** e **hora de término** para definir o intervalo de tempo dos dados a serem incluídos nos arquivos de log.

Se você selecionar um período de tempo muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de log pode se tornar muito grande para ser armazenado em um nó ou muito grande para ser coletado para o nó de administração principal para download. Se isso ocorrer, você deve reiniciar a coleta de logs com um conjunto menor de dados.

4. Selecione os tipos de registros que pretende recolher.

- **Logs de aplicativos:** Logs específicos de aplicativos que o suporte técnico utiliza com mais frequência para solução de problemas. Os registros recolhidos são um subconjunto dos registros de aplicações disponíveis.
- **Logs de auditoria:** Logs contendo as mensagens de auditoria geradas durante a operação normal do sistema.
- **Rastreamento de rede:** Logs usados para depuração de rede.
- **Prometheus Database:** Métricas de séries temporais dos serviços em todos os nós.

5. Opcionalmente, insira notas sobre os arquivos de log que você está reunindo na caixa de texto * Notas*.

Você pode usar essas notas para fornecer informações de suporte técnico sobre o problema que o levou a coletar os arquivos de log. Suas anotações são adicionadas a um arquivo `info.txt` chamado ,

juntamente com outras informações sobre a coleção de arquivos de log. O `info.txt` ficheiro é guardado no pacote de arquivo de registo.

6. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.

7. Selecione **Collect Logs**.

Quando você envia uma nova solicitação, a coleção anterior de arquivos de log é excluída.

Você pode usar a página Logs para monitorar o progresso da coleção de arquivos de log para cada nó de grade.

Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo menor ou por menos nós.

8. Selecione **Download** quando a coleção de arquivos de log estiver concluída.

O arquivo `.tar.gz` contém todos os arquivos de log de todos os nós de grade onde a coleta de log foi bem-sucedida. Dentro do arquivo combinado `.tar.gz`, há um arquivo de log para cada nó de grade.

Depois de terminar

Você pode baixar novamente o pacote de arquivo de log mais tarde, se precisar.

Opcionalmente, você pode selecionar **Excluir** para remover o pacote de arquivo de log e liberar espaço em disco. O pacote de arquivo de log atual é removido automaticamente da próxima vez que você coletar arquivos de log.

Acione manualmente um pacote AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente um pacote AutoSupport a ser enviado.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você deve ter a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT > Tools > AutoSupport**.
2. Na guia **ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

O StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.

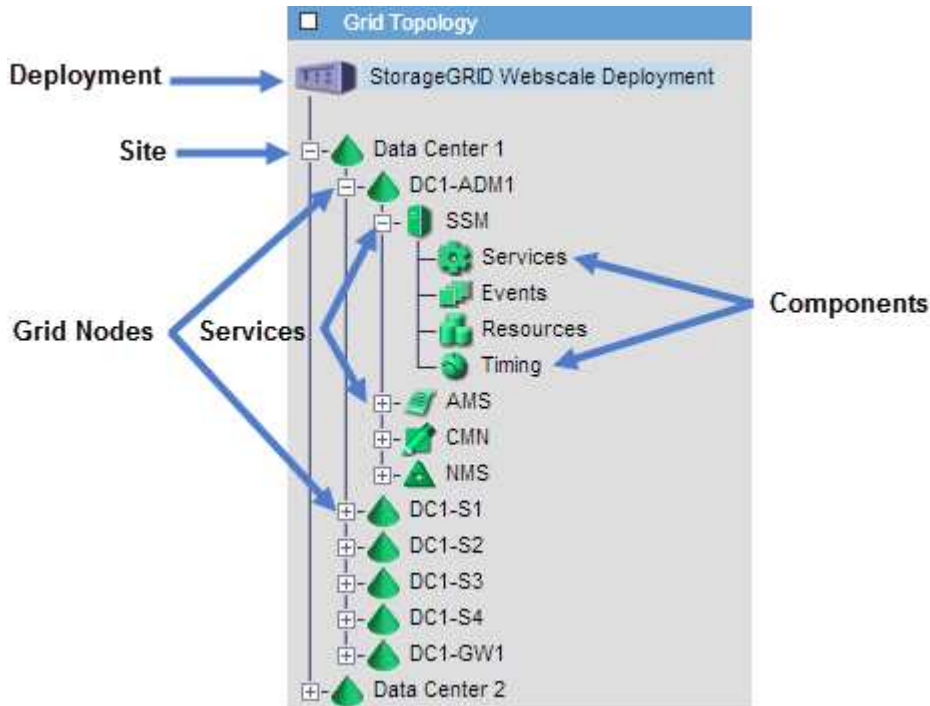


Depois de enviar um pacote AutoSupport acionado pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Veja a árvore de topologia de Grade

A árvore de topologia de grade fornece acesso a informações detalhadas sobre elementos do sistema StorageGRID, incluindo sites, nós de grade, serviços e componentes. Na maioria dos casos, você só precisa acessar a árvore de topologia de grade quando instruído na documentação ou quando estiver trabalhando com suporte técnico.

Para acessar a árvore de topologia de grade, selecione **SUPPORT > Tools > Grid topology**.



Para expandir ou recolher a árvore de topologia de Grade, clique **+** ou no local, nó ou **-** nível de serviço. Para expandir ou recolher todos os itens em todo o site ou em cada nó, mantenha pressionada a tecla **<Ctrl>** e clique em.

Atributos do StorageGRID

Atributos reportam valores e status para muitas das funções do sistema StorageGRID. Os valores de atributo estão disponíveis para cada nó de grade, cada local e toda a grade.

Os atributos do StorageGRID são usados em vários lugares no Gerenciador de Grade:

- **Página de nós:** Muitos dos valores mostrados na página de nós são atributos StorageGRID. (As métricas Prometheus também são mostradas nas páginas de nós.)
- **Alarmes:** Quando os atributos atingem valores de limite definidos, os alarmes StorageGRID (sistema legado) são acionados em níveis de gravidade específicos.
- **Grid Topology tree:** Os valores de atributo são mostrados na árvore Grid Topology (**SUPPORT > Tools > Grid topology**).
- **Eventos:** Os eventos do sistema ocorrem quando certos atributos Registram uma condição de erro ou falha para um nó, incluindo erros como erros de rede.

Valores de atributo

Os atributos são reportados com o melhor esforço e estão aproximadamente corretos. As atualizações de atributos podem ser perdidas em algumas circunstâncias, como a falha de um serviço ou a falha e reconstrução de um nó de grade.

Além disso, os atrasos de propagação podem retardar o relatório de atributos. Os valores atualizados para a maioria dos atributos são enviados para o sistema StorageGRID em intervalos fixos. Pode demorar vários minutos até que uma atualização seja visível no sistema, e dois atributos que mudam mais ou menos simultaneamente podem ser reportados em momentos ligeiramente diferentes.

Análise as métricas de suporte

Ao solucionar um problema, você pode trabalhar com suporte técnico para analisar métricas e gráficos detalhados do seu sistema StorageGRID.

Antes de começar

- Você deve estar conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#)tem .

Sobre esta tarefa

A página Metrics permite que você acesse as interfaces de usuário Prometheus e Grafana. Prometheus é um software de código aberto para coletar métricas. Grafana é um software de código aberto para visualização de métricas.



As ferramentas disponíveis na página Metrics destinam-se a ser utilizadas pelo suporte técnico. Alguns recursos e itens de menu dentro dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Consulte a lista ["Métricas de Prometheus comumente usadas"](#) de .

Passos

1. Conforme indicado pelo suporte técnico, selecione **SUPPORT > Tools > Metrics**.

Um exemplo da página Metrics é mostrado aqui:

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- [https://\[redacted\]](https://[redacted])

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	

2. Para consultar os valores atuais das métricas do StorageGRID e visualizar gráficos dos valores ao longo do tempo, clique no link na seção Prometheus.

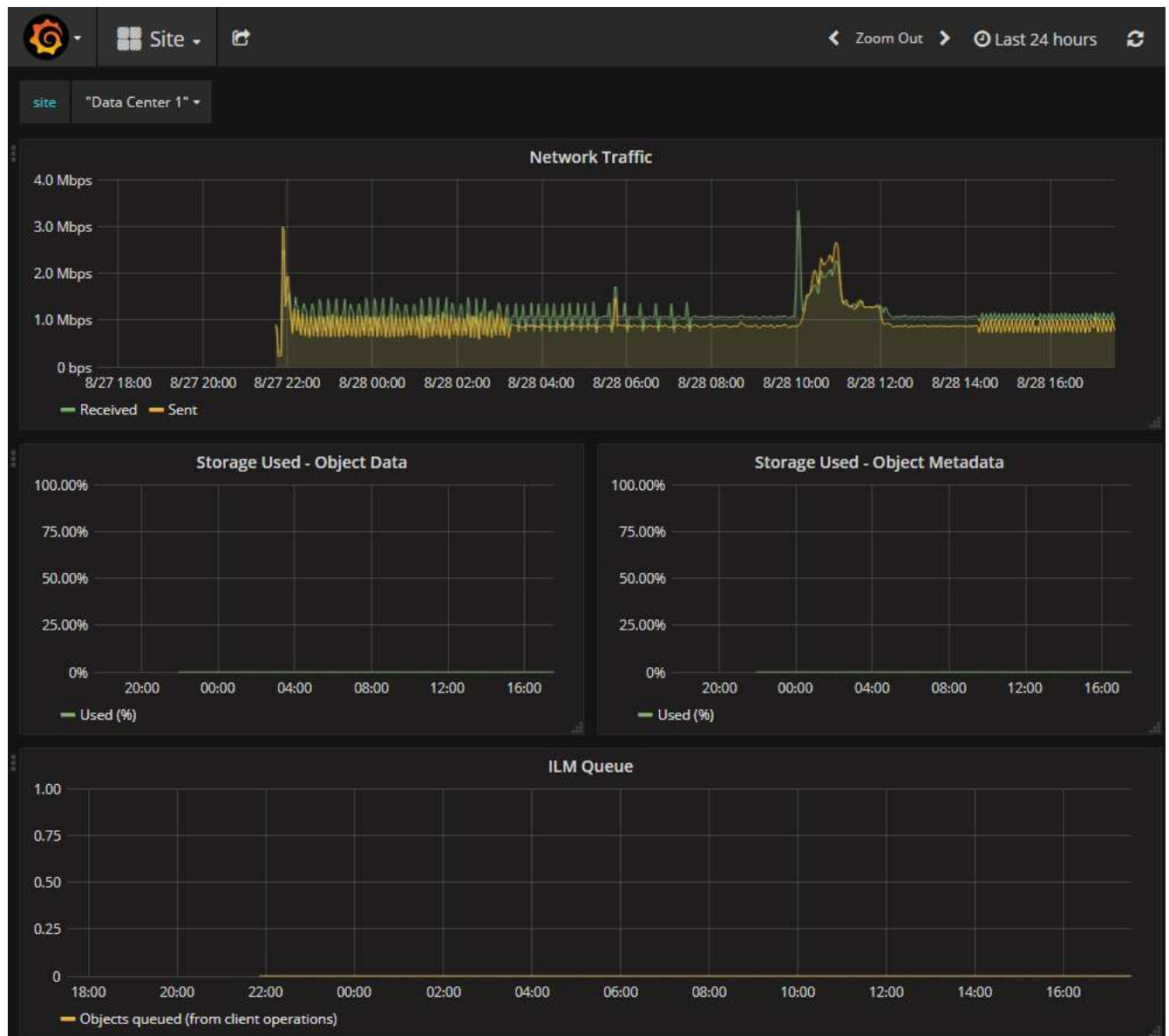
A interface Prometheus é exibida. Você pode usar essa interface para executar consultas sobre as métricas disponíveis do StorageGRID e para traçar métricas do StorageGRID ao longo do tempo.



As métricas que incluem *private* em seus nomes são destinadas apenas para uso interno e estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

3. Para acessar painéis pré-construídos contendo gráficos de métricas do StorageGRID ao longo do tempo, clique nos links na seção Grafana.

A interface Grafana para o link selecionado é exibida.



Execute o diagnóstico

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no sistema StorageGRID e analisar os resultados.




- ["Analise as métricas de suporte"](#)
- ["Métricas de Prometheus comumente usadas"](#)

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você ["permissões de acesso específicas"](#)tem .

Sobre esta tarefa

A página Diagnósticos executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um de três Estados:

-  **Normal:** Todos os valores estão dentro do intervalo normal.
-  **Atenção:** Um ou mais valores estão fora do intervalo normal.
-  **Atenção:** Um ou mais dos valores estão significativamente fora do intervalo normal.

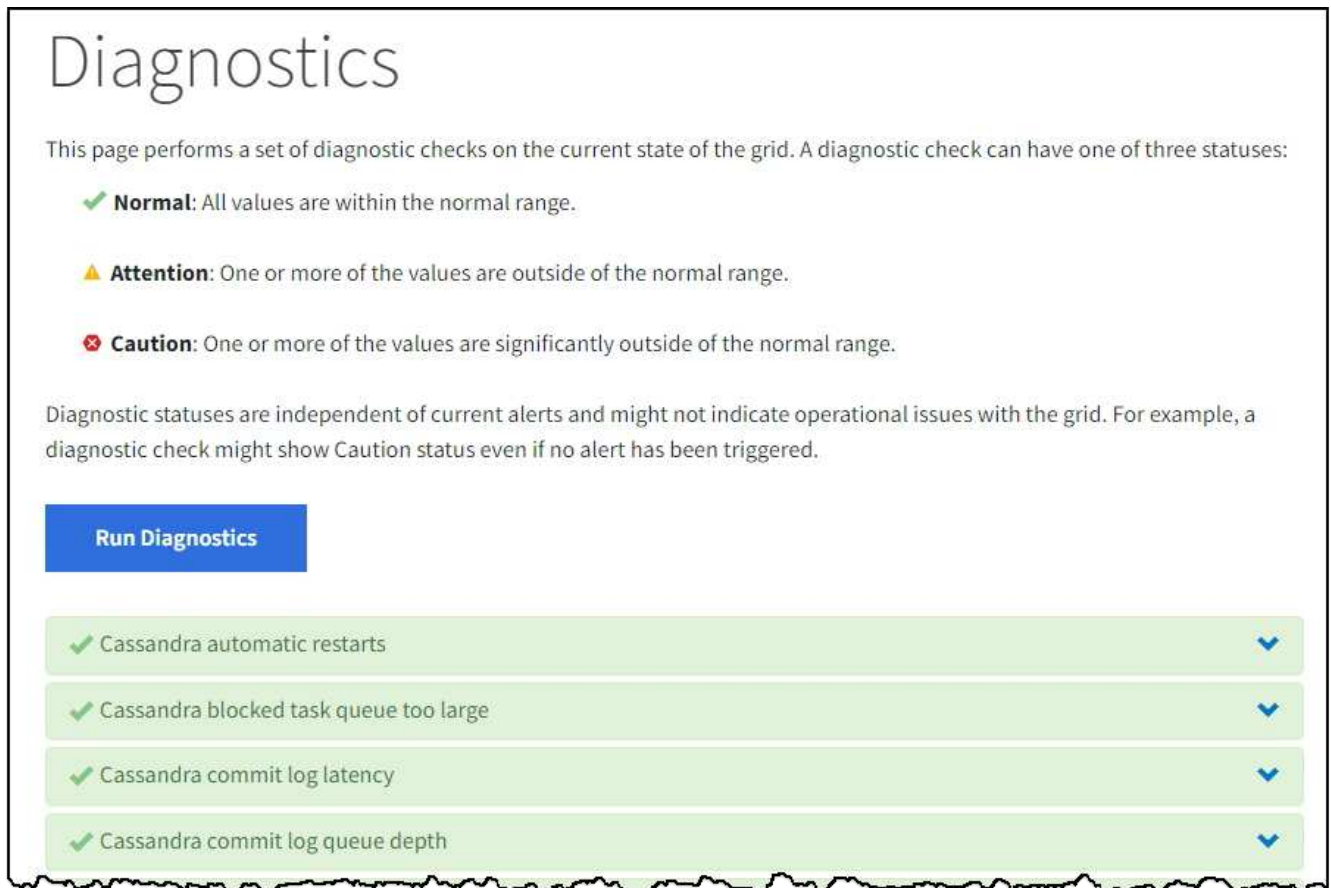
Os Estados de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a grade. Por exemplo, uma verificação de diagnóstico pode mostrar o estado de precaução mesmo que nenhum alerta tenha sido acionado.

Passos

1. Selecione **SUPPORT > Tools > Diagnostics**.

A página Diagnósticos é exibida e lista os resultados de cada verificação de diagnóstico. Os resultados são classificados por gravidade (cuidado, atenção e, em seguida, normal). Dentro de cada gravidade, os resultados são ordenados alfabeticamente.

Neste exemplo, todos os diagnósticos têm um estado normal.



Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✗ **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

[Run Diagnostics](#)

- ✓ Cassandra automatic restarts
- ✓ Cassandra blocked task queue too large
- ✓ Cassandra commit log latency
- ✓ Cassandra commit log queue depth

2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

São apresentados detalhes sobre o diagnóstico e os seus resultados atuais. Os seguintes detalhes são listados:

- **Status:** O estado atual deste diagnóstico: Normal, atenção ou cuidado.
- **Consulta Prometheus:** Se usada para o diagnóstico, a expressão Prometheus que foi usada para

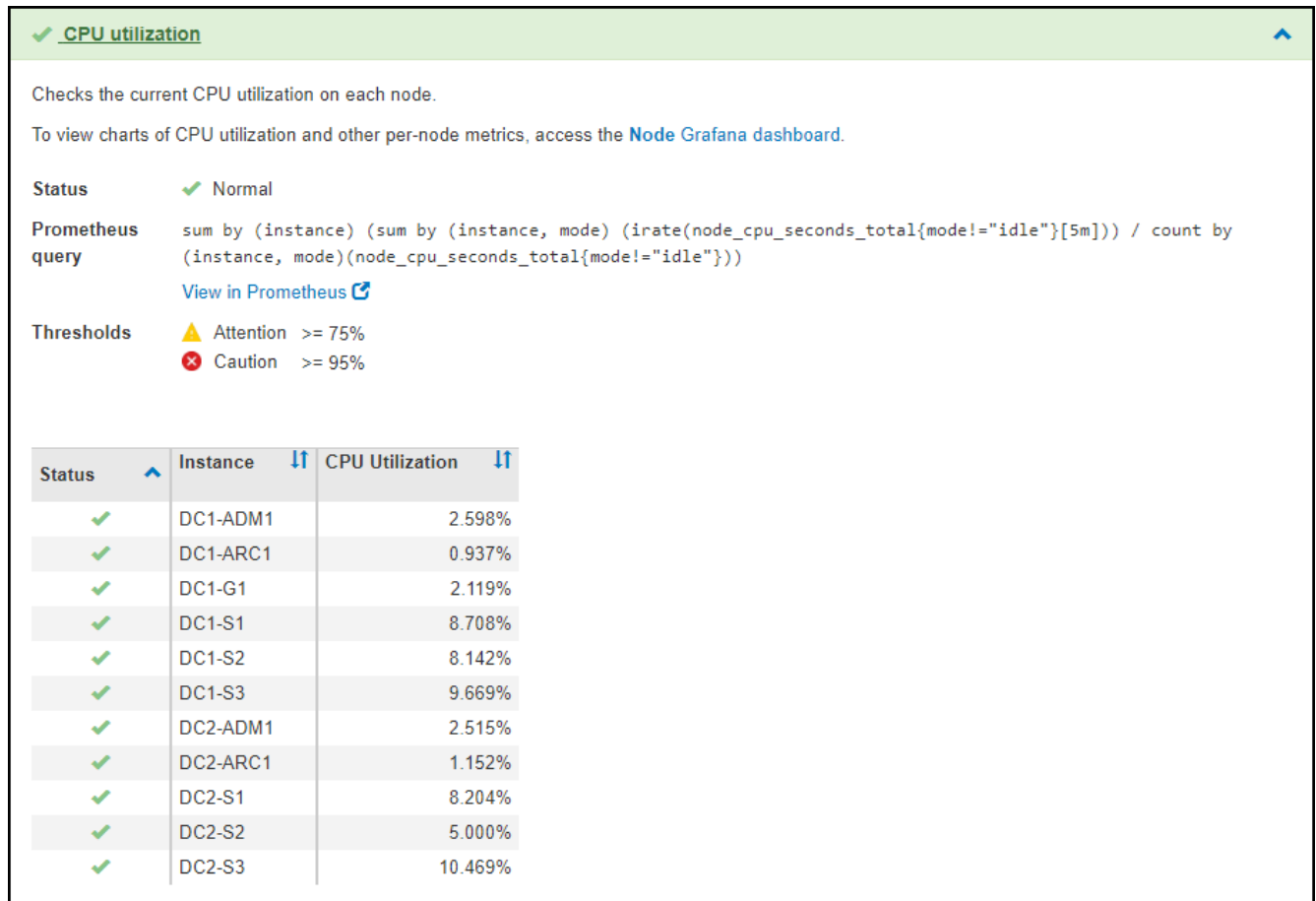
gerar os valores de status. (Uma expressão Prometheus não é usada para todos os diagnósticos.)

- **Limiares:** Se disponíveis para o diagnóstico, os limiares definidos pelo sistema para cada estado de diagnóstico anormal. (Os valores de limite não são usados para todos os diagnósticos.)



Não é possível alterar esses limites.

- **Valores de estado:** Uma tabela que mostra o estado e o valor do diagnóstico em todo o sistema StorageGRID. Neste exemplo, a utilização atual da CPU para cada nó em um sistema StorageGRID é mostrada. Todos os valores de nós estão abaixo dos limites de atenção e cuidado, portanto, o status geral do diagnóstico é normal.



3. **Opcional:** Para ver gráficos do Grafana relacionados a este diagnóstico, clique no link **painel do Grafana**.

Este link não é exibido para todos os diagnósticos.

O painel do Grafana relacionado é exibido. Neste exemplo, o painel Node aparece mostrando a utilização da CPU ao longo do tempo para este nó, bem como outros gráficos Grafana para o nó.



Você também pode acessar os painéis Grafana pré-construídos na seção Grafana da página **SUPPORT > Tools > Metrics**.



4. **Opcional:** Para ver um gráfico da expressão Prometheus ao longo do tempo, clique em **Exibir em Prometheus**.

Aparece um gráfico Prometheus da expressão usada no diagnóstico.

☐ Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

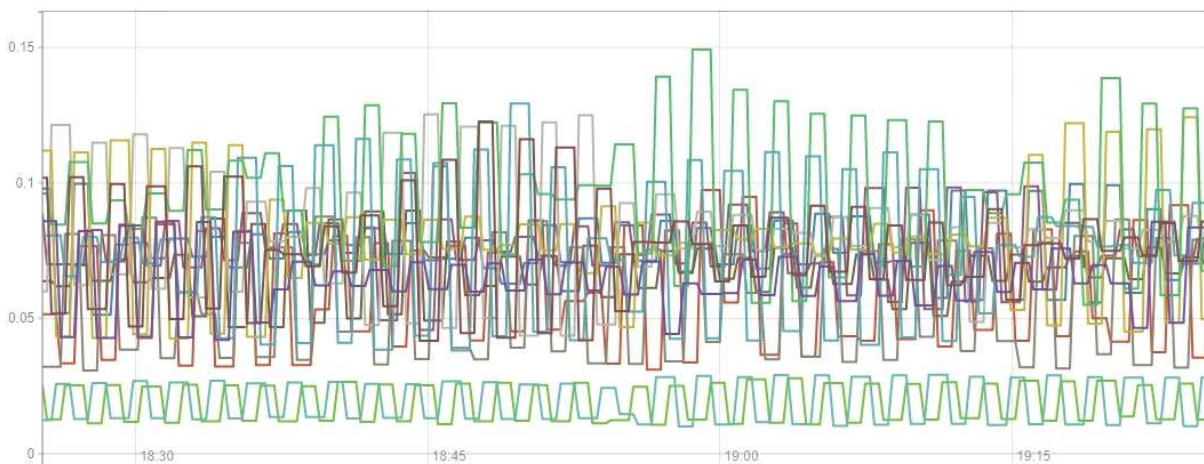
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor - ▾

Graph Console

1h ⏪ Until ⏩ Res. (s) ☐ stacked



- ✓ {instance="DC3-S3"}
- ✓ {instance="DC3-S2"}
- ✓ {instance="DC3-S1"}
- ✓ {instance="DC2-S3"}
- ✓ {instance="DC2-S2"}
- ✓ {instance="DC2-S1"}
- ✓ {instance="DC2-ADM1"}
- ✓ {instance="DC1-S3"}
- ✓ {instance="DC1-S2"}
- ✓ {instance="DC1-S1"}
- ✓ {instance="DC1-G1"}
- ✓ {instance="DC1-ARC1"}
- ✓ {instance="DC1-ADM1"}

Remove Graph

Add Graph

Crie aplicativos de monitoramento personalizados

Você pode criar aplicativos e painéis de monitoramento personalizados usando as métricas do StorageGRID disponíveis na API de gerenciamento de grade.

Se você quiser monitorar métricas que não são exibidas em uma página existente do Gerenciador de Grade ou se quiser criar painéis personalizados para o StorageGRID, use a API de Gerenciamento de Grade para consultar métricas do StorageGRID.

Você também pode acessar métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como Grafana. O uso de uma ferramenta externa requer que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Consulte ["Instruções para administrar o StorageGRID"](#).

Para exibir as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Gerenciador de Grade. Na parte superior da página, selecione o ícone de ajuda e selecione **Documentação da API > métricas**.



GET	<code>/grid/metric-labels/{label}/values</code>	Lists the values for a metric label	
GET	<code>/grid/metric-names</code>	Lists all available metric names	
GET	<code>/grid/metric-query</code>	Performs an instant metric query at a single point in time	
GET	<code>/grid/metric-query-range</code>	Performs a metric query over a range of time	

Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo desta documentação.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. 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 SOBRESSALIENTES; 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 DESTES SOFTWARES, 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.