



Monitorar e manter o StorageGRID

StorageGRID

NetApp
March 12, 2025

Índice

Monitorar e manter o StorageGRID	1
Monitorar e solucionar problemas	1
Monitorar e solucionar problemas: Visão geral	1
Veja o Dashboard	1
Exibir a página nós	5
Informações que você deve monitorar regularmente	40
Gerencie alertas e alarmes	74
Configurar mensagens de auditoria e destinos de log	121
Use um servidor syslog externo	126
Utilize a monitorização SNMP	141
Colete dados adicionais do StorageGRID	156
Solucionar problemas de um sistema StorageGRID	191
Referência de alertas	260
Métricas de Prometheus comumente usadas	298
Referência de alarmes (sistema legado)	304
Referência de ficheiros de registo	335
Expanda sua grade	353
Expanda sua grade: Visão geral	354
Planeje a expansão do StorageGRID	355
Reúna os materiais necessários	368
Adicione volumes de armazenamento	375
Adicione nós de grade ou local	384
Configurar o sistema expandido	400
Entre em Contato com o suporte técnico	409
Recuperar e manter	410
Recuperar e manter: Visão geral	410
Procedimento de correção do StorageGRID	411
Procedimentos de recuperação do nó de grade	420
Como a recuperação do local é realizada pelo suporte técnico	533
Procedimento de desativação	535
Procedimentos de manutenção da rede	592
Procedimentos de nível de host e middleware	619
Procedimentos do nó de grade	628
Clonagem do nó do dispositivo	653
Rever registos de auditoria	662
Revisar logs de auditoria: Visão geral	662
Faça auditoria de arquivos de log e formatos de mensagens	666
Auditar mensagens e o ciclo de vida do objeto	685
Auditar mensagens	693

Monitorar e manter o StorageGRID

Monitorar e solucionar problemas

Monitorar e solucionar problemas: Visão geral

Use estas instruções para monitorar um sistema StorageGRID e avaliar e resolver problemas que possam ocorrer.

Sobre estas instruções

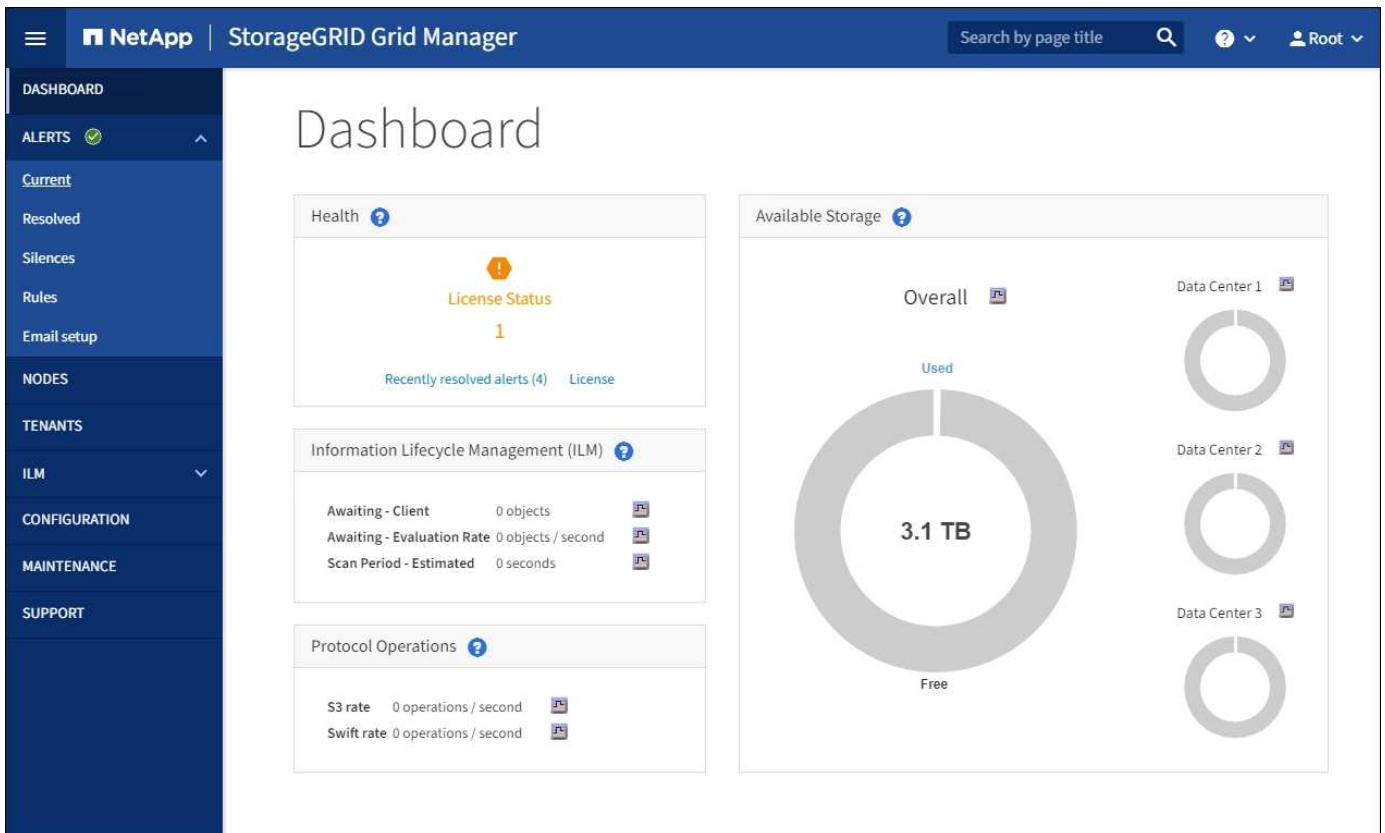
Estas instruções descrevem como usar o Gerenciador de Grade para monitorar um sistema StorageGRID. Você aprenderá quais informações você deve monitorar regularmente, como gerenciar alertas e alarmes legados, como usar o SNMP para monitoramento e como obter dados adicionais do StorageGRID, incluindo métricas e diagnósticos.

Essas instruções também descrevem como solucionar problemas de um sistema StorageGRID e descrever todos os alertas do sistema, alarmes legados e arquivos de log.

Use estas instruções se você estiver monitorando e apoiando um sistema StorageGRID depois que ele for instalado.

Veja o Dashboard

Ao iniciar sessão pela primeira vez no Gestor de grelha, pode utilizar o Painel para monitorizar rapidamente as atividades do sistema. O Dashboard inclui informações sobre integridade do sistema, métricas de uso e tendências e gráficos operacionais.




Campo de pesquisa

O campo **Search** na barra de cabeçalho permite que você navegue rapidamente para uma página específica ou entrada da barra lateral dentro do Gerenciador de Grade. Por exemplo, você pode inserir **key** para acessar a página Key Management Server.

Painel de saúde

Descrição	Veja detalhes adicionais	Saiba mais
<p>Resume a saúde do sistema. Uma marca de seleção verde significa que não há alertas atuais e todos os nós de grade estão conectados. Qualquer outro ícone significa que há pelo menos um alerta atual ou nó desconectado.</p>	<p>Você pode ver um ou mais dos seguintes links:</p> <ul style="list-style-type: none"> • Detalhes da grade: Aparece se algum nó estiver desconectado (estado de conexão desconhecido ou administrativamente inativo). Clique no link ou clique no ícone azul ou cinza para determinar que nó ou nós são afetados. • Alertas atuais: Aparece se algum alerta estiver ativo no momento. Clique no link ou clique em Crítica, Principal ou menor para ver os detalhes na página ALERTAS atual. • Alertas resolvidos recentemente: Aparece se algum alerta acionado na semana passada estiver resolvido. Clique no link para ver os detalhes na página ALERTAS resolvidos. • Alarms Legacy: Aparece se algum alarme (sistema legado) estiver ativo no momento. Clique no link para ver os detalhes na página SUPORTE Alarmes (legado) Alarmes atuais. • Licença: Aparece se houver um problema com a licença de software para este sistema StorageGRID. Clique no link para ver os detalhes na página MANUTENÇÃO sistema Licença. 	<ul style="list-style-type: none"> • Monitorar os estados de conexão do nó • Ver alertas atuais • Exibir alertas resolvidos • Ver alarmes legados • Administrar o StorageGRID

Painel de armazenamento disponível

Descrição	Veja detalhes adicionais	Saiba mais
<p>Exibe a capacidade de armazenamento disponível e usada em toda a grade, não incluindo Mídia de arquivamento.</p> <p>O gráfico geral apresenta totais em toda a grade. Se esta for uma grade de vários locais, gráficos adicionais serão exibidos para cada local do data center.</p> <p>Você pode usar essas informações para comparar o armazenamento usado com o armazenamento disponível. Se você tem uma grade de vários locais, você pode determinar qual site está consumindo mais armazenamento.</p>	<ul style="list-style-type: none"> • Para visualizar a capacidade, coloque o cursor sobre as seções de capacidade disponível e usada do gráfico. • Para exibir tendências de capacidade em um intervalo de datas, clique no ícone de gráfico  da grade geral ou em um local de data center. • Para ver detalhes, selecione NÓS. Em seguida, exiba a guia Storage (armazenamento) para toda a grade, um site inteiro ou um nó de armazenamento único. 	<ul style="list-style-type: none"> • Exibir a guia armazenamento • Monitorar a capacidade de armazenamento

Painel ILM (Information Lifecycle Management)

Descrição	Veja detalhes adicionais	Saiba mais
<p>Exibe as operações ILM atuais e as filas ILM para o seu sistema. Você pode usar essas informações para monitorar a carga de trabalho do sistema.</p> <ul style="list-style-type: none"> • Aguardando - Cliente: O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest). • Aguardando - taxa de avaliação: A taxa atual na qual os objetos são avaliados em relação à política ILM na grade. • Período de digitalização - estimado: O tempo estimado para concluir uma varredura ILM completa de todos os objetos. Nota: Uma verificação completa não garante que o ILM tenha sido aplicado a todos os objetos. 	<ul style="list-style-type: none"> • Para ver detalhes, selecione NÓS. Em seguida, exiba a guia ILM para toda a grade, um site inteiro ou um nó de armazenamento único. • Para ver as regras existentes do ILM, selecione ILM Rules. • Para ver as políticas ILM existentes, selecione ILM Policies. 	<ul style="list-style-type: none"> • Veja a guia ILM • Administrar o StorageGRID.

Painel Protocol Operations (operações de protocolo)

Descrição	Veja detalhes adicionais	Saiba mais
<p>Exibe o número de operações específicas do protocolo (S3 e Swift) executadas pelo seu sistema.</p> <p>Use essas informações para monitorar os workloads e a eficiência do sistema. As taxas de protocolo são médias nos últimos dois minutos.</p>	<ul style="list-style-type: none">• Para ver detalhes, selecione NÓS. Em seguida, exiba a guia objetos para toda a grade, um site inteiro ou um nó de armazenamento único.• Para ver tendências ao longo de um intervalo de datas, clique no ícone de gráfico à direita da taxa de protocolo S3 ou Swift.	<ul style="list-style-type: none">• Exibir a guia objetos• Use S3• Use Swift


Exibir a página nós

Quando você precisar de informações mais detalhadas sobre 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.

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%
DC2	Site	0%	0%	—


A tabela nós lista todos os sites e nós no seu sistema StorageGRID. As informações de resumo são exibidas para cada nó. Se um nó 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.

Ícones de estado da ligação

- **Não conetado - desconhecido** : o nó não está conetado à grade por um motivo desconhecido. Por exemplo, a conexão de rede entre nós foi perdida ou a energia está inativa. O alerta **não é possível se comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.






Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.

- **Não conetado - administrativamente para baixo** : o nó não está conetado à grade por um motivo esperado. Por exemplo, o nó, ou serviços no nó, foi desligado graciosamente, o nó está reiniciando ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.

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

Ícones de alerta

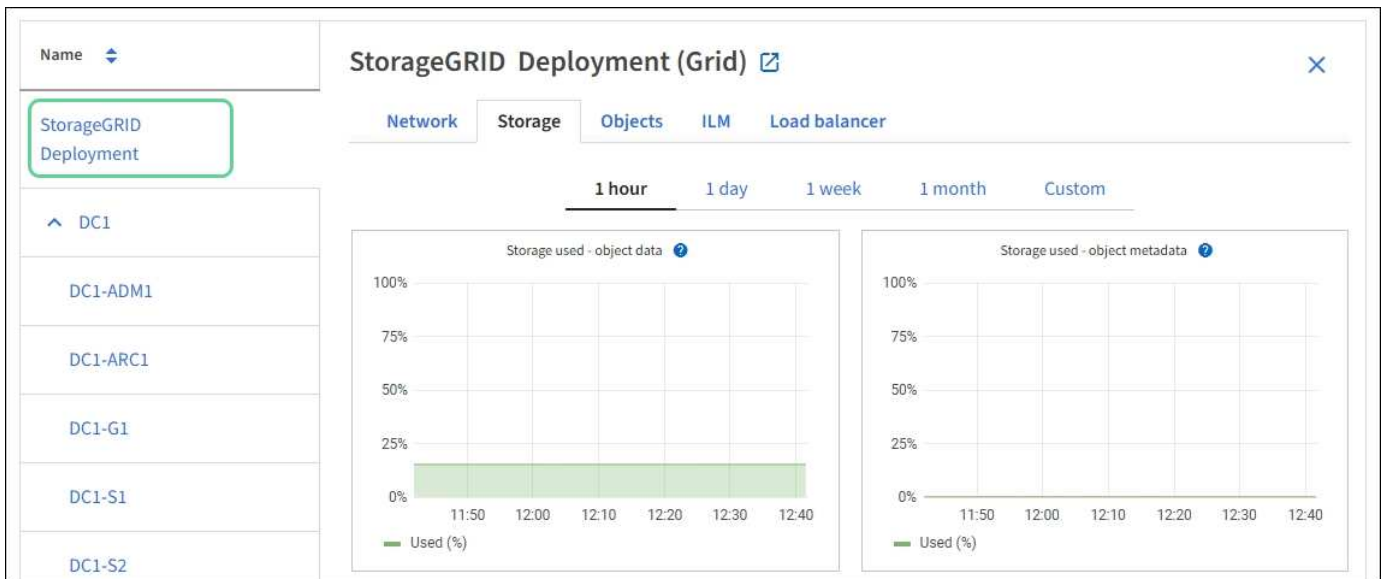
Se houver um alerta ativo para um nó, um dos seguintes ícones será exibido ao lado do nome do nó:

- **Crítico** : existe uma condição anormal que interrompeu as operações normais de um nó ou serviço StorageGRID. Você deve abordar o problema subjacente imediatamente. A interrupção do serviço e a perda de dados podem resultar se o problema não for resolvido.
- **Major** : existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não pare a operação normal de um nó ou serviço StorageGRID.
- **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.

Exibindo detalhes de um sistema, site ou nó

Para exibir as informações disponíveis, selecione o nome da grade, do site ou do nó da seguinte forma:

- 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.



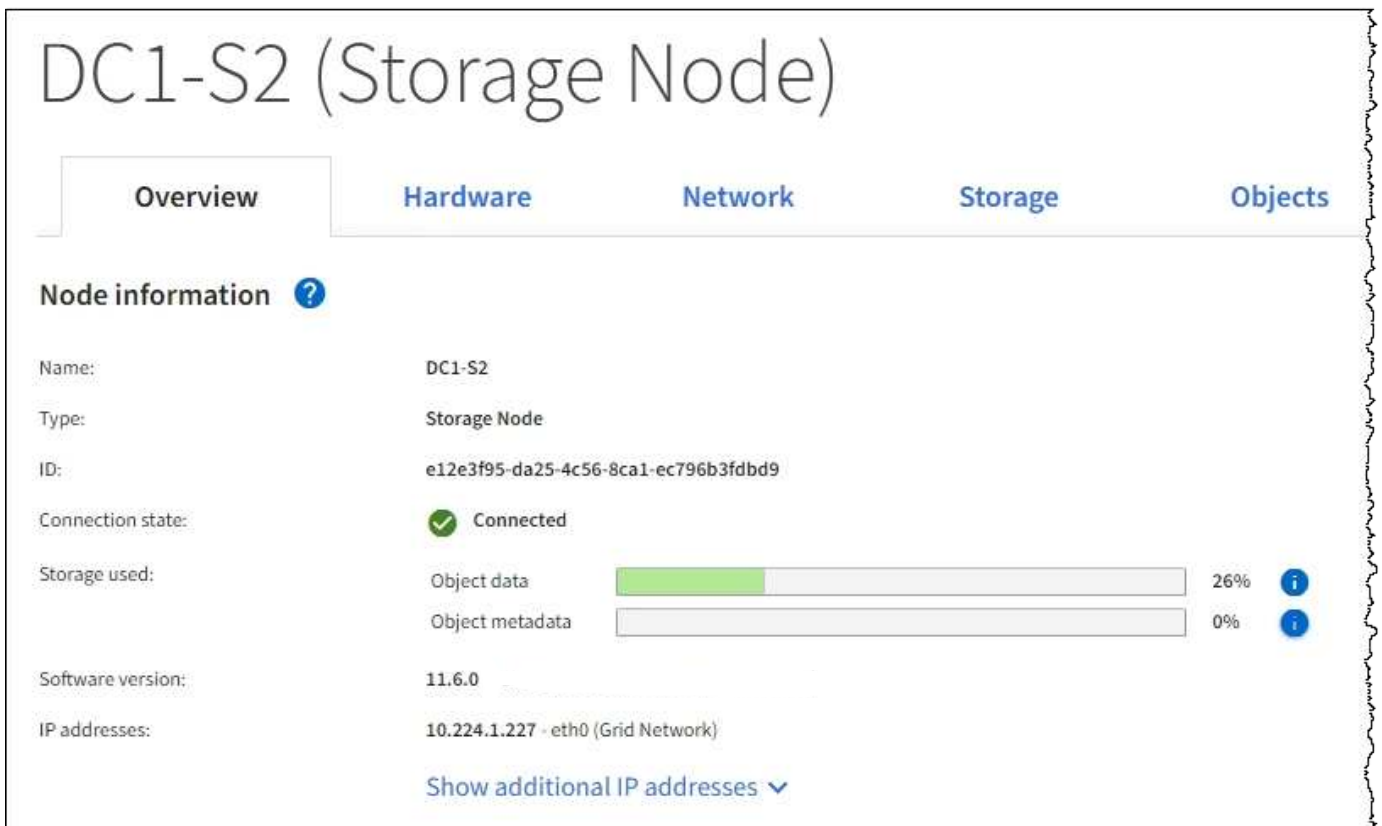
Veja a guia Visão geral

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 da grade.





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

- **Nome:** O nome do host atribuído ao nó e exibido no Gerenciador de Grade.
- **Tipo:** O tipo de nó — nó Admin, nó Admin primário, nó de armazenamento, nó de gateway ou nó de arquivo.
- **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** : o nó não está conectado à grade por um motivo desconhecido. Por exemplo, a conexão de rede entre nós foi perdida ou a energia está inativa. O alerta **não é possível se comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.



Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.

- **Administrativamente para baixo** : o nó não está 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 todos os alertas que atualmente afetam esse nó que não foram silenciados. Clique no nome do alerta para ver detalhes adicionais e ações recomendadas.

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

Informações relacionadas

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

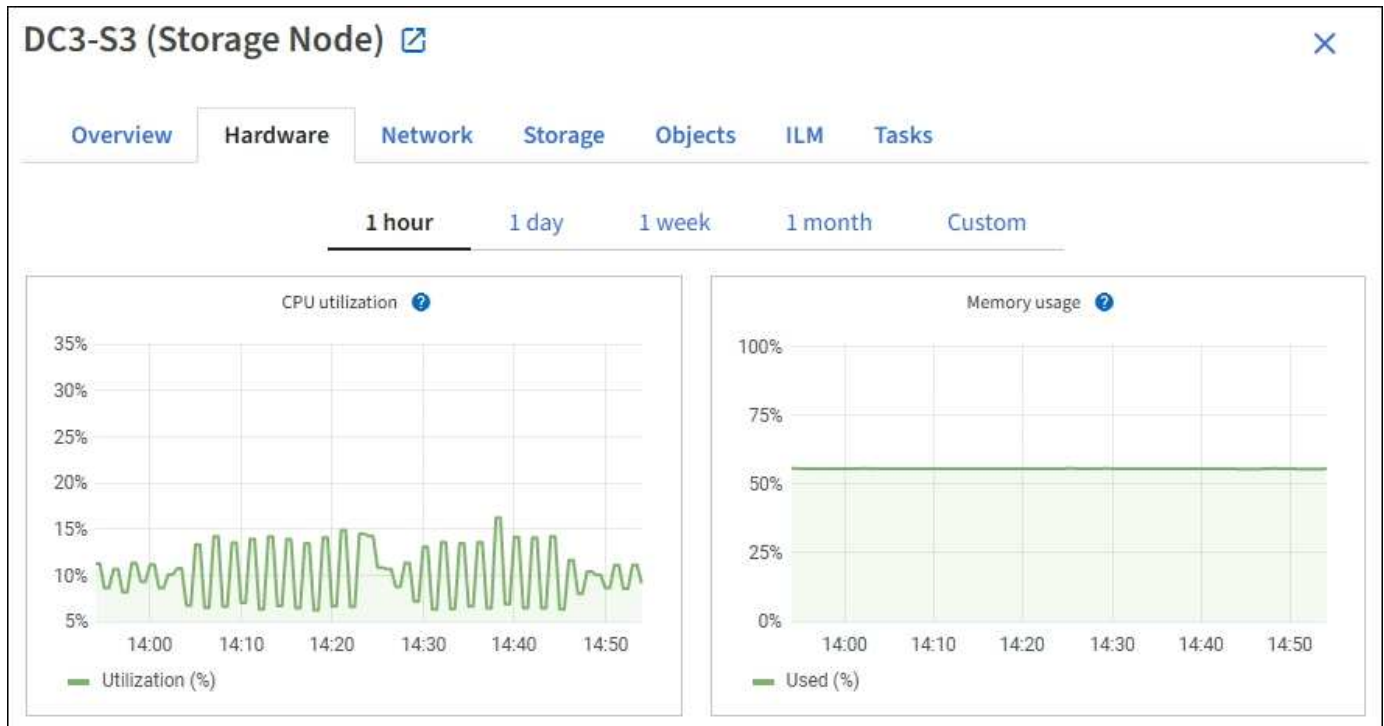
[Ver alertas atuais](#)

[Veja um alerta específico](#)

Exibir a guia hardware

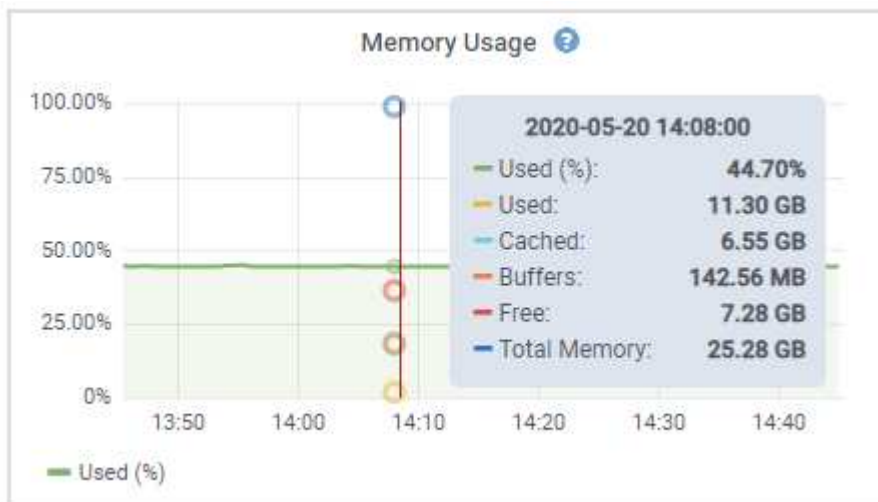
A guia hardware exibe a utilização da CPU e o uso da memória para cada nó e informações adicionais de hardware sobre dispositivos.

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, passe 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.

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

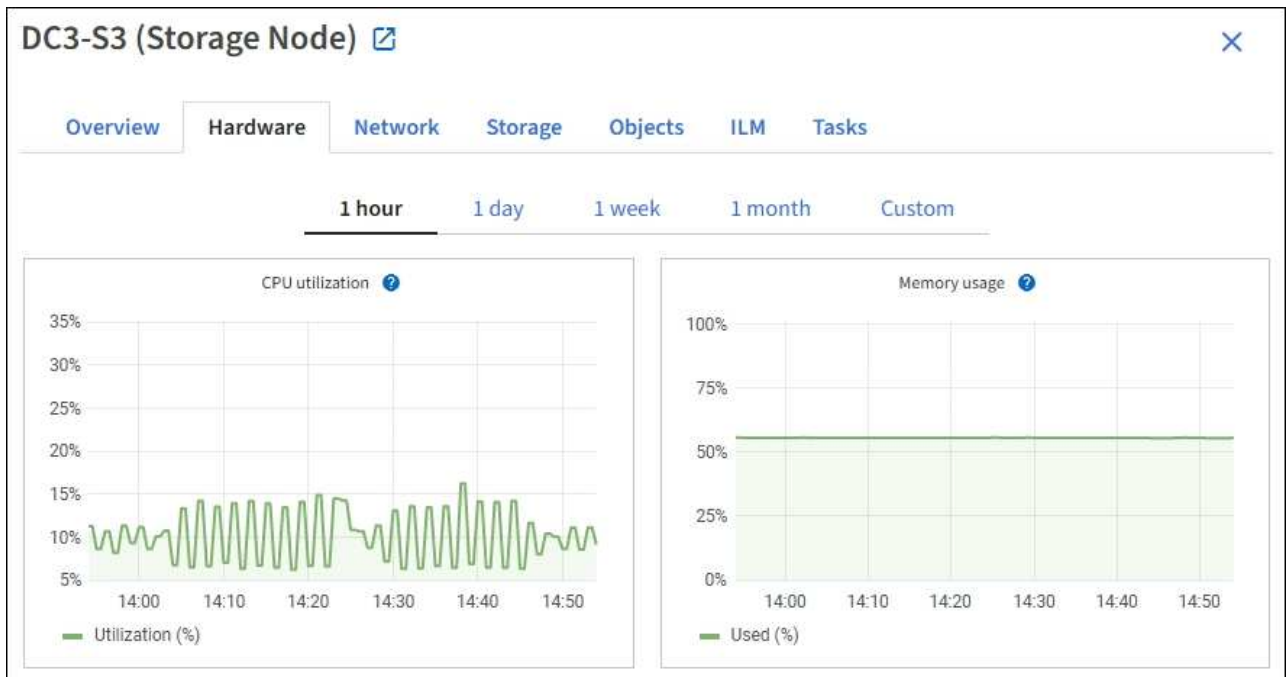
Alerts

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.

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











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



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

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

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 software SANtricity.
Nome do controlador de storage	O nome deste dispositivo StorageGRID mostrado no software SANtricity.
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 software SANtricity 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 software SANtricity 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 software SANtricity.
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 software SANtricity. 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 estado 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 (unidade de disco rígido) ou SSD (unidade de estado sólido).

Campo na mesa do aparelho	Descrição
Tamanho da unidade de dados de armazenamento	O tamanho efetivo de uma unidade de dados. Nota: Para nós com compartimentos de expansão, use o Tamanho da unidade de dados para cada gaveta em vez disso. O tamanho efetivo da unidade pode ser diferente por gaveta.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de storage	O estado de conectividade de storage.
Fonte de alimentação geral	O estado de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento de placa base (BMC) no controlador de computação. Você usa esse IP para se conectar à interface do BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é apresentado para modelos de aparelhos que não contêm um BMC.
Número de série do controlador de computação	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação. Esse campo não é exibido para modelos de dispositivo que não têm hardware de computação e hardware de storage 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 SG6060X.</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.

4. Confirme se todos os Estados são ""nominais"".

Se um status não for "nominal", revise os 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.

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

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



1. 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

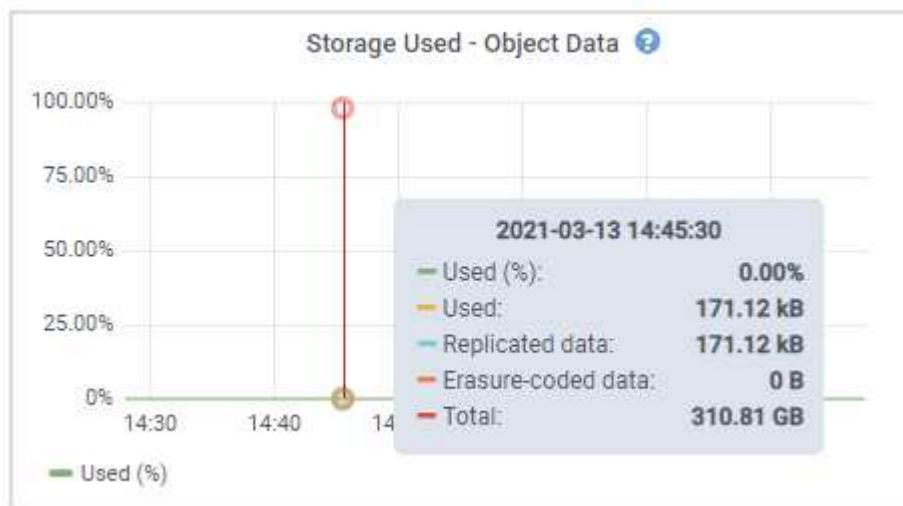
Consulte as instruções de instalação e manutenção do seu dispositivo para obter mais informações sobre como configurar as portas 10/25-GbE.

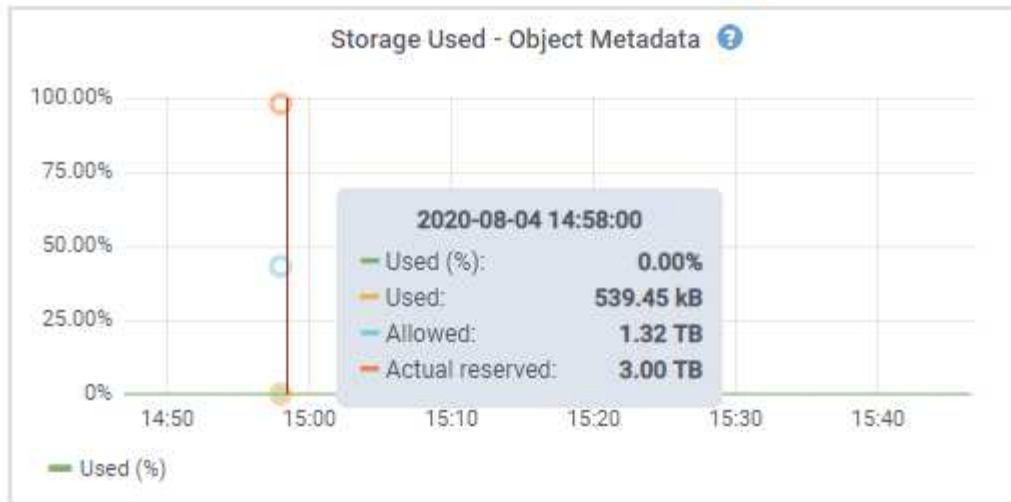
2. Reveja a secção Comunicação de rede.

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	

3. Seleccione **armazenamento** para visualizar gráficos que mostram as percentagens 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 software SANtricity (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

Informações relacionadas

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG5600 dispositivos de armazenamento](#)

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

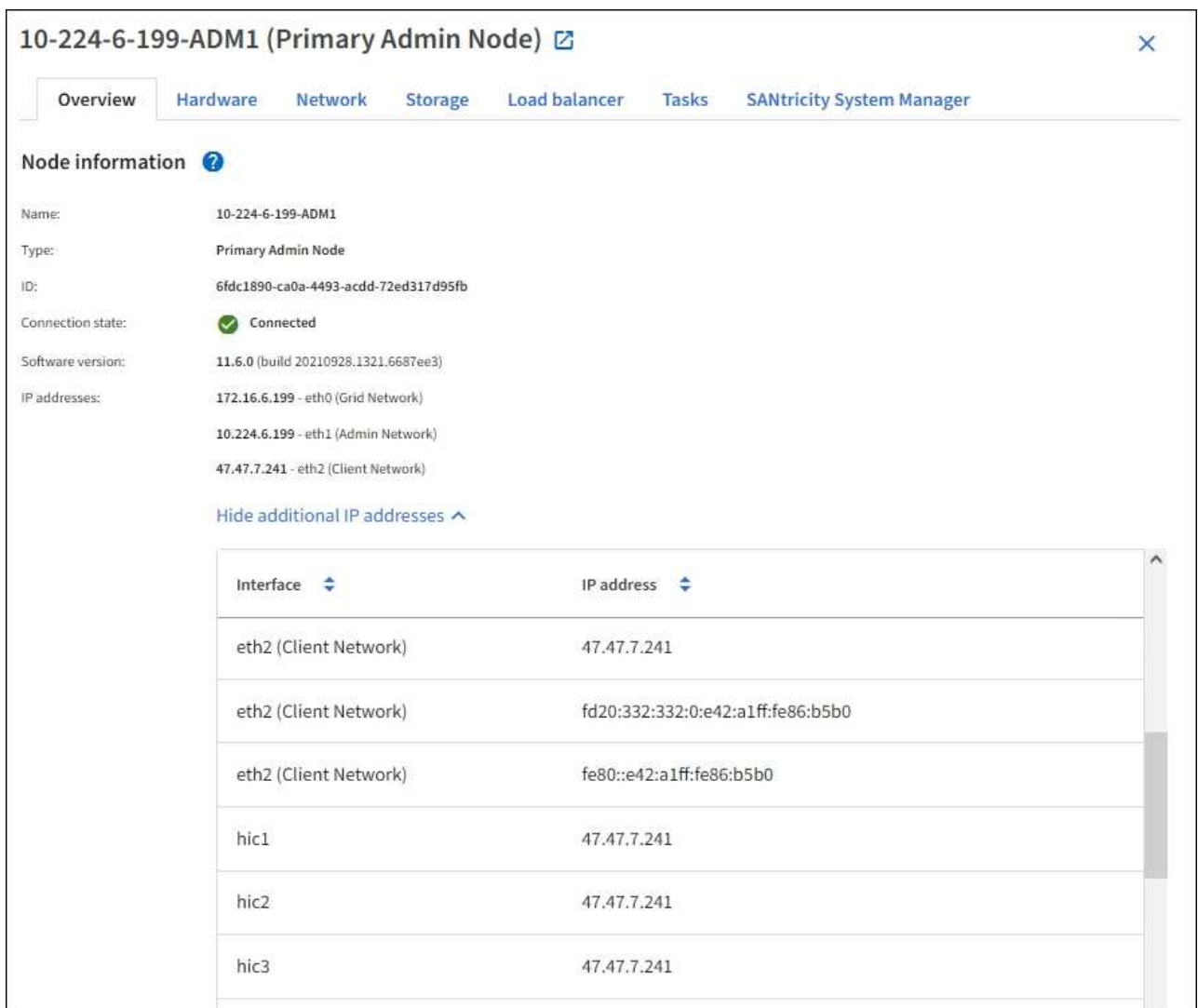
A página nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada dispositivo de serviços que é usado como nó de administrador ou nó de gateway. Você também pode ver memória, hardware de armazenamento, recursos de rede, interfaces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

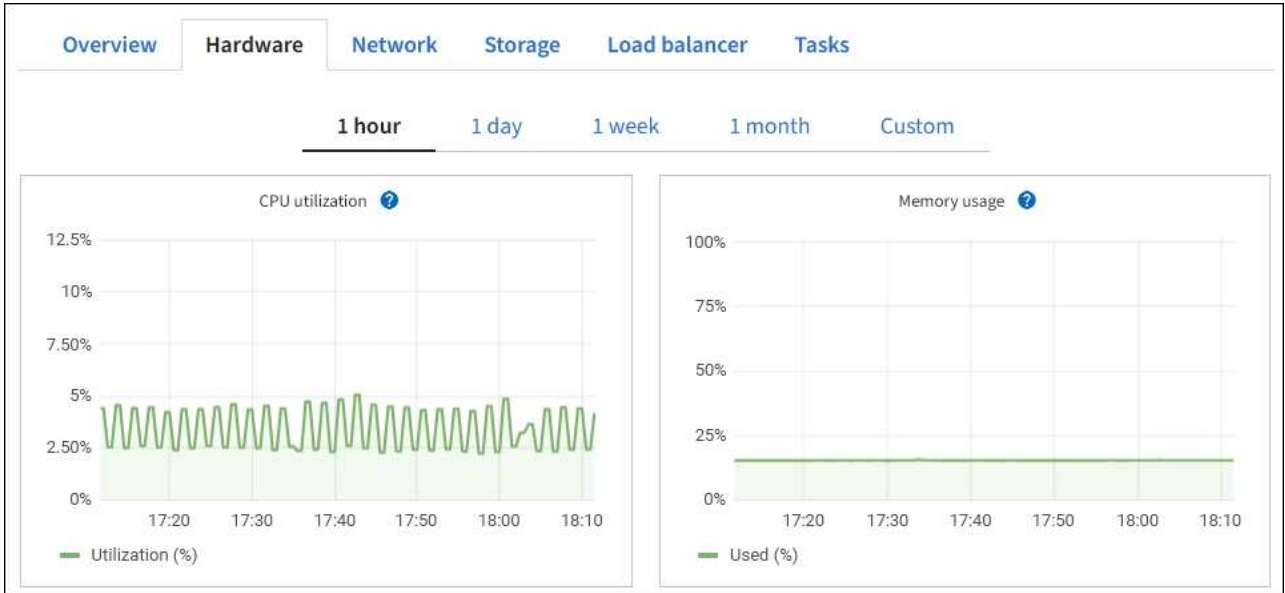
[Hide additional IP addresses](#)

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.

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



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

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

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

Se um status não for "nominal", revise os 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.

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Load balancer](#)[Tasks](#)

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

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

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

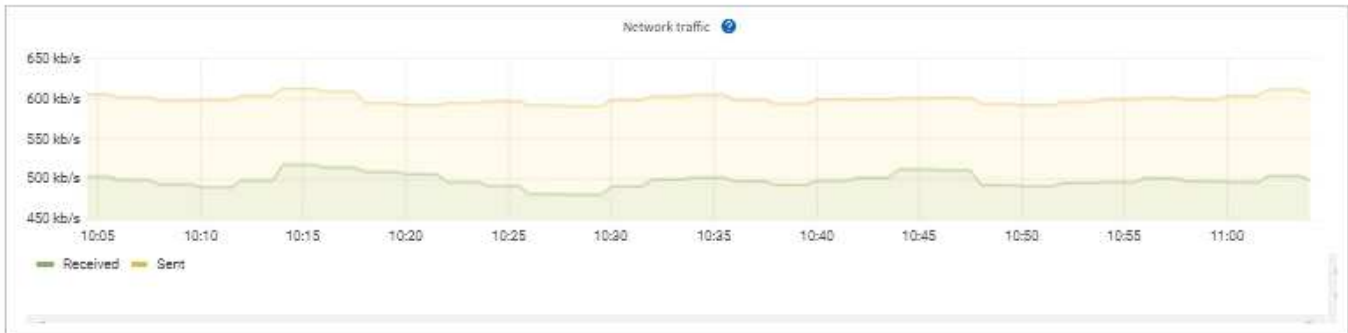
1 hour

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.

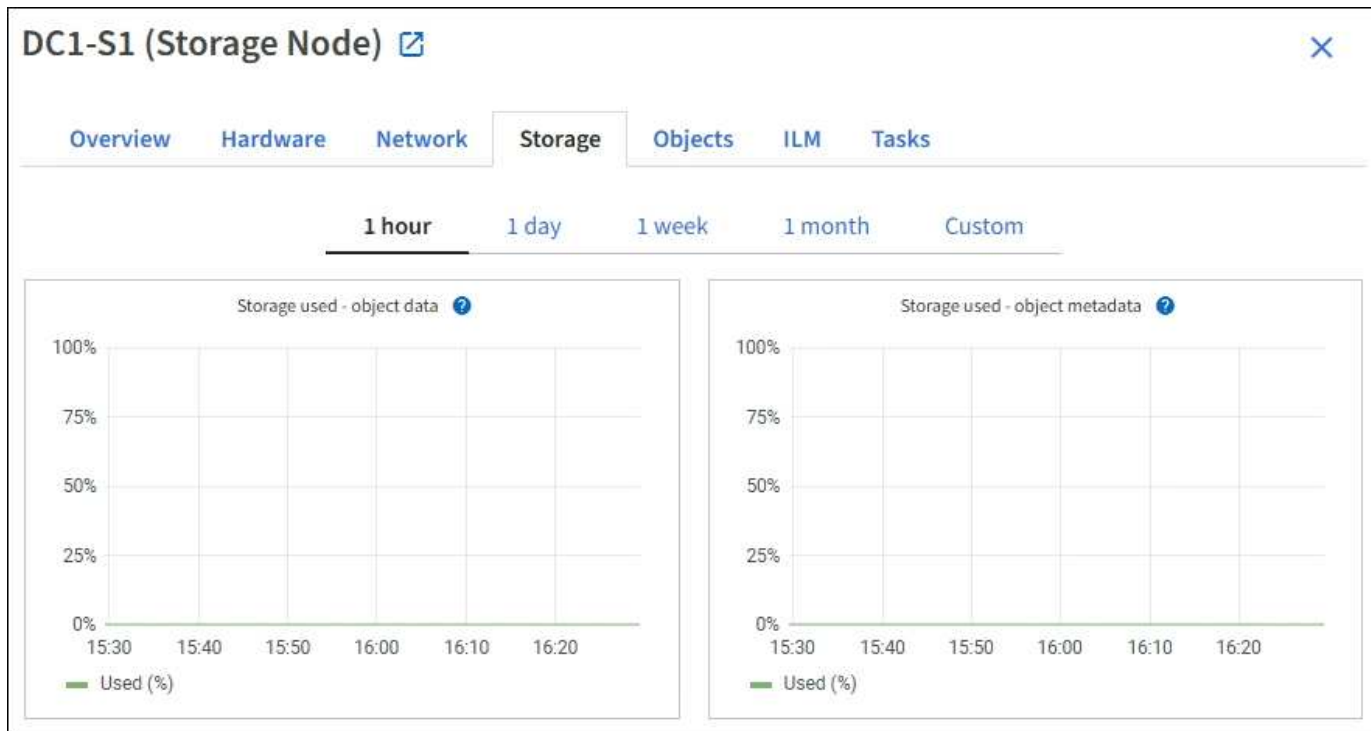
A guia Storage (armazenamento) é exibida para todos os nós, cada local e toda a grade.

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.



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



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](#)

Use a guia tarefa para reinicializar um nó de grade

A guia tarefa permite reinicializar o nó selecionado. A guia tarefa é mostrada para todos os nós.

O que você vai precisar

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

- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Você pode usar a guia tarefa para reinicializar um nó. Para nós de dispositivo, você também pode usar a guia tarefa para colocar o dispositivo no modo de manutenção.

- Reiniciar um nó de grade a partir da guia tarefa emite o comando reboot no nó de destino. Quando você reinicia um nó, o nó é encerrado e reinicia. Todos os serviços são reiniciados automaticamente.

Se você planeja reinicializar um nó de armazenamento, observe o seguinte:

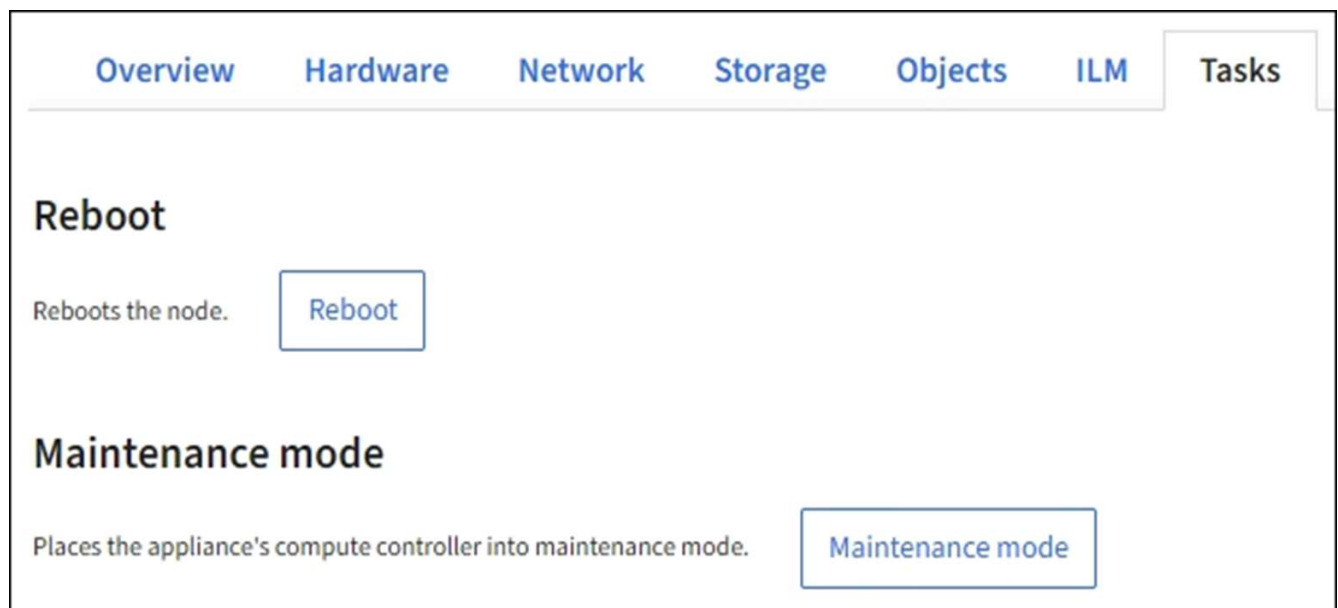
- Se uma regra ILM especificar um comportamento de ingestão de confirmação dupla ou a regra especificar balanceado e não for possível criar imediatamente todas as cópias necessárias, o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo local e avaliará o ILM posteriormente. Se você quiser reinicializar dois ou mais nós de storage em um determinado site, talvez não seja possível acessar esses objetos durante a reinicialização.
- Para garantir que você possa acessar todos os objetos enquanto um nó de armazenamento estiver reiniciando, pare de ingerir objetos em um site por aproximadamente uma hora antes de reiniciar o nó.
- Talvez seja necessário colocar um dispositivo StorageGRID no modo de manutenção para executar determinados procedimentos, como alterar a configuração do link ou substituir um controlador de armazenamento. Para obter instruções, consulte as instruções de instalação e manutenção do equipamento.



Em casos raros, colocar um dispositivo StorageGRID no modo de manutenção pode tornar o dispositivo indisponível para acesso remoto.

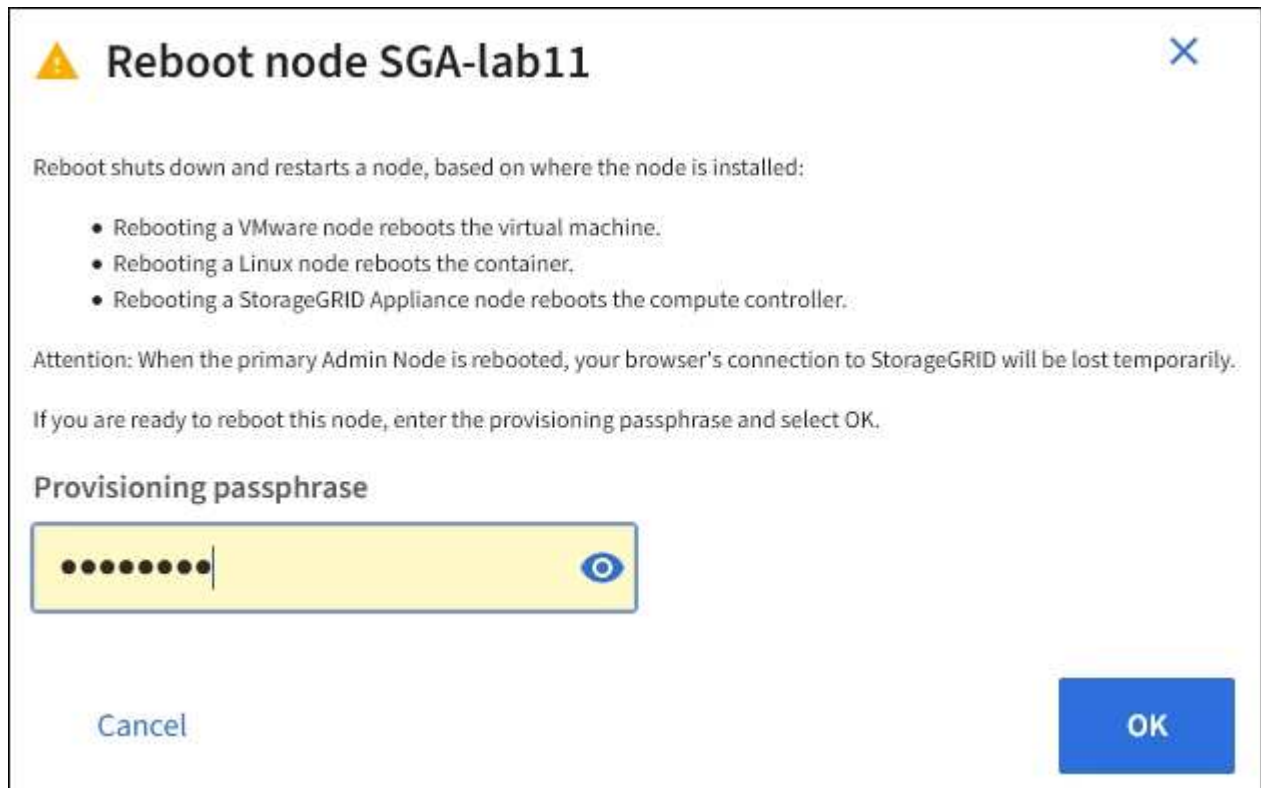
Passos

1. Selecione **NODES**.
2. Selecione o nó de grade que deseja reinicializar.
3. Selecione a guia **tarefas**.



4. Selecione **Reboot**.

É apresentada uma caixa de diálogo de confirmação.



Se você estiver reinicializando o nó Admin principal, a caixa de diálogo de confirmação lembra que a conexão do seu navegador com o Gerenciador de Grade será perdida temporariamente quando os serviços forem interrompidos.

5. Digite a senha de provisionamento e clique em **OK**.

6. Aguarde até que o nó seja reiniciado.

Pode levar algum tempo para que os serviços sejam desativados.

Quando o nó é reinicializado, o ícone cinza (administrativamente para baixo) aparece no lado esquerdo da página **nodes**. Quando todos os serviços forem iniciados novamente e o nó for conectado com êxito à grade, a página **nós** deve exibir um status normal (sem ícones à esquerda do nome do nó), indicando que nenhum alerta está ativo e o nó está conectado à grade.

Informações relacionadas

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG5600 dispositivos de armazenamento](#)

[Aparelhos de serviços SG100 e SG1000](#)

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 do Information Lifecycle Management (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 de apagamento.

DC2-S1 (Storage Node) [↗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) **ILM** [Tasks](#)

Evaluation

Awaiting - all: ?	0 objects	
Awaiting - client: ?	0 objects	
Evaluation rate: ?	0.00 objects / second	
Scan rate: ?	0.00 objects / second	

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-09-09 17:36:44 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Informações relacionadas

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

[Administrar o StorageGRID](#)

Veja a guia Load Balancer (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 ""nenhum dado".



Solicitar tráfego

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



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

Taxa de solicitação recebida

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

Duração média da solicitação (sem erro)

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

Taxa de resposta de erro

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

Informações relacionadas

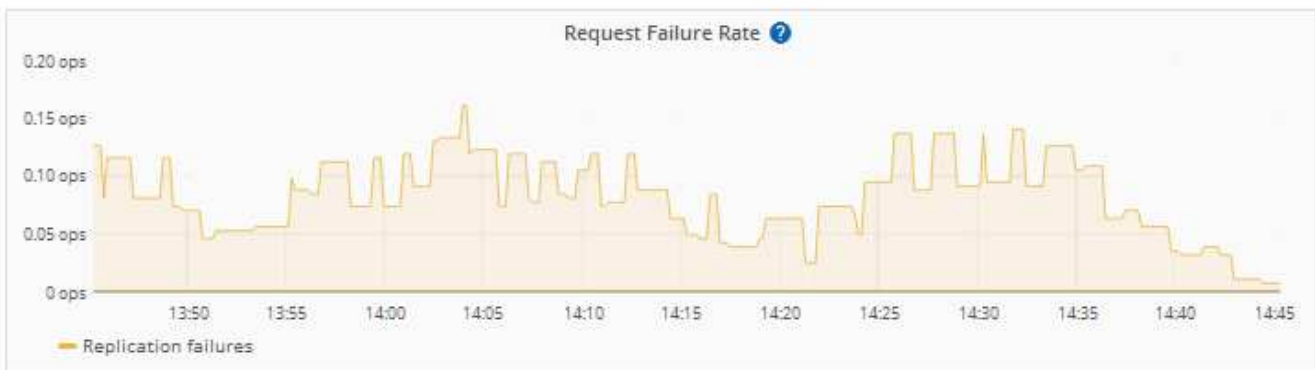
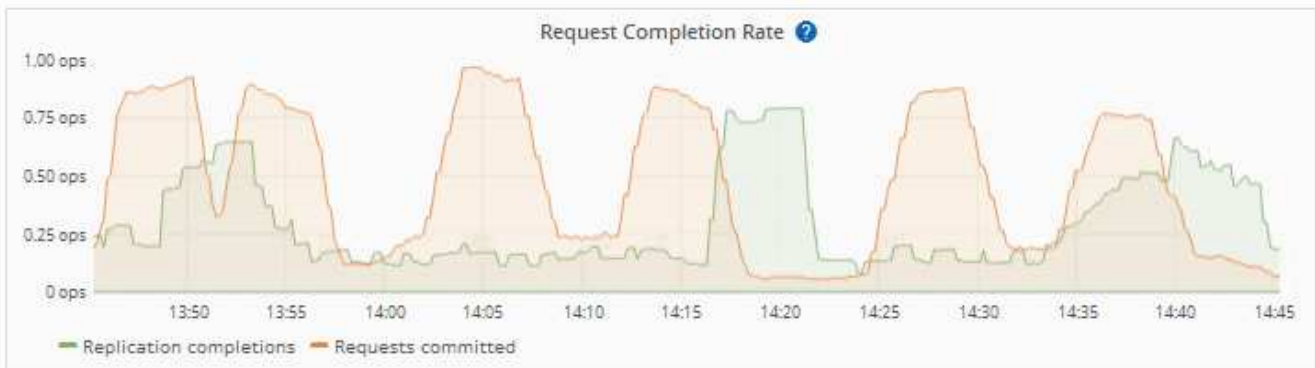
[Monitorar operações de balanceamento de carga](#)

[Administrar o StorageGRID](#)

Veja a guia Serviços da Plataforma

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

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



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

Veja a guia Gerenciador do sistema do SANtricity

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 para os nós de dispositivos de storage.

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 sistemas do SANtricity para configurar um proxy para o e-Series AutoSupport, consulte as instruções em como administrar o StorageGRID.

Administrar o StorageGRID

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



Você deve ter o firmware SANtricity 8,70 (11,70) ou superior para acessar o Gerenciador de sistema SANtricity usando o Gerenciador de Grade.



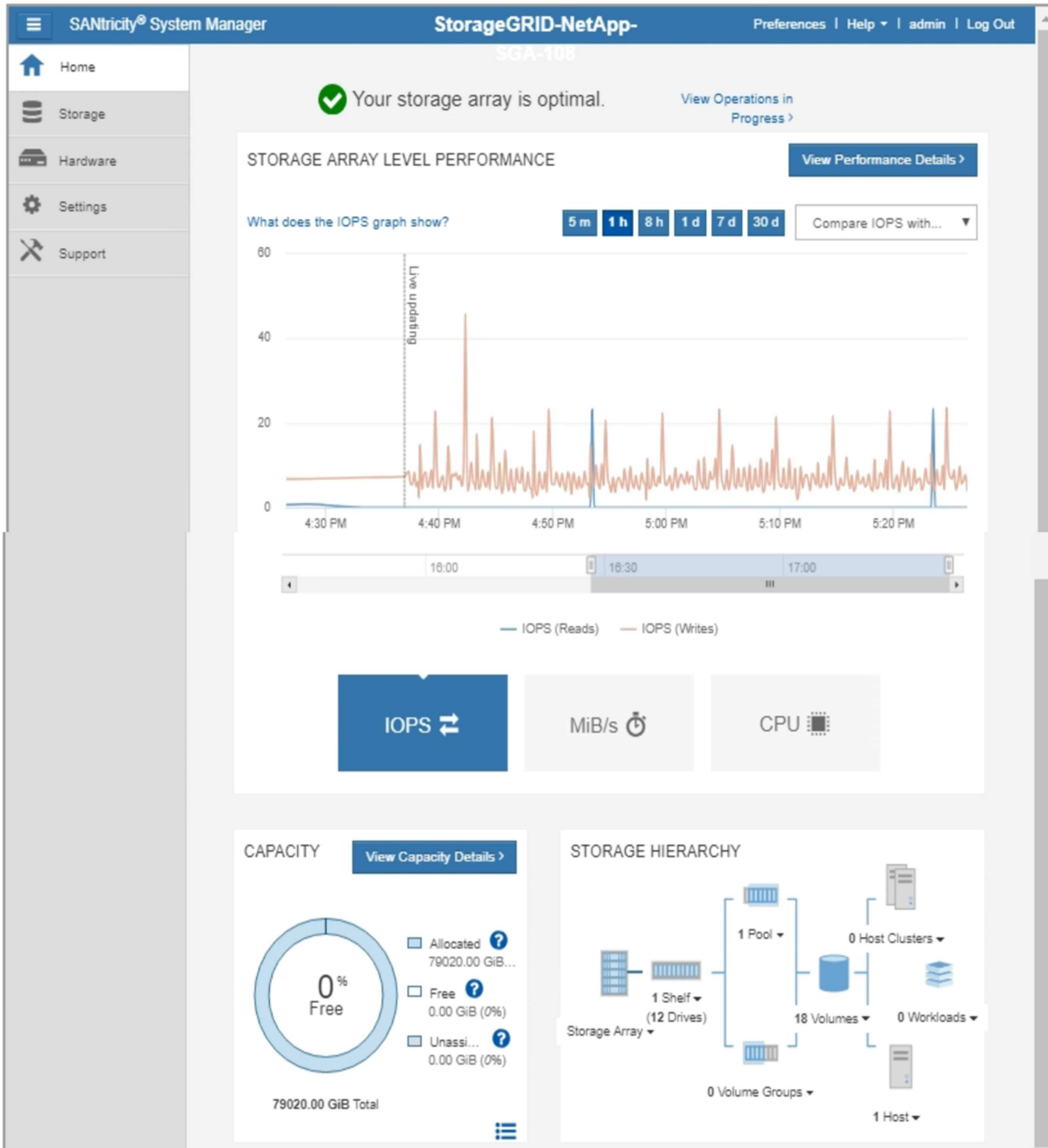
O acesso ao Gerenciador de sistemas do SANtricity a partir do Gerenciador de Grade geralmente se destina apenas a monitorar o hardware do dispositivo e configurar o e-Series AutoSupport. Muitos recursos e operações no Gerenciador de sistemas do SANtricity, como atualização de firmware, não se aplicam ao monitoramento do dispositivo StorageGRID. Para evitar problemas, siga sempre as instruções de instalação e manutenção do 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, passe 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 que você deve monitorar regularmente

O StorageGRID é um sistema de storage distribuído e tolerante a falhas que foi projetado para continuar operando mesmo quando ocorrem erros ou quando nós ou sites não estão disponíveis. Você precisa monitorar proativamente a integridade do sistema, os workloads e as estatísticas de uso, para que você possa agir para solucionar possíveis problemas antes que eles afetem a eficiência ou a disponibilidade da grade.

Um sistema ocupado gera grandes quantidades de informações. Esta seção fornece orientações sobre as informações mais importantes a monitorizar de forma contínua.

O que monitorar	Frequência
O dados de integridade do sistema mostrado no Painel do Gerenciador de Grade. Observe se alguma coisa mudou do dia anterior.	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
Conexões de rede e desempenho	Semanalmente
Recursos em nível de nó	Semanalmente
Atividade do locatário	Semanalmente
Capacidade do sistema de armazenamento de arquivos externo	Semanalmente
Operações de balanceamento de carga	Após a configuração inicial e após quaisquer alterações de configuração
Disponibilidade de hotfixes de software e atualizações de software	Mensalmente

Monitorar a integridade do sistema

Você deve monitorar diariamente a integridade geral do seu sistema StorageGRID.

Sobre esta tarefa

O sistema StorageGRID é tolerante a falhas e pode continuar a funcionar mesmo quando partes da grade não estão disponíveis. O primeiro sinal de um possível problema com o seu sistema StorageGRID é provavelmente um alerta ou um alarme (sistema legado) e não necessariamente um problema com as operações do sistema. Prestar atenção à integridade do sistema pode ajudá-lo a detectar problemas menores

antes que eles afetem as operações ou a eficiência da rede.

O painel Saúde no Painel do Gerenciador de Grade fornece um resumo dos problemas que podem estar afetando o sistema. Você deve investigar quaisquer problemas que são mostrados no Dashboard.



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

Passos

1. Faça login no Gerenciador de Grade para exibir o Dashboard.
2. Reveja as informações no painel Saúde.



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

Link	Indica
Detalhes da grelha	Aparece se algum nó estiver desconetado (estado de conexão desconhecido ou administrativamente inativo). Clique no link ou clique no ícone azul ou cinza para determinar que nó ou nós são afetados.
Alertas atuais	Aparece se algum alerta estiver ativo no momento. Clique no link ou clique em Crítica , Principal ou menor para ver os detalhes na página ALERTAS atual .
Alertas resolvidos recentemente	Aparece se quaisquer alertas acionados na semana passada estiverem agora resolvidos. Clique no link para ver os detalhes na página ALERTAS resolvidos .
Licença	É apresentado se existir um problema com a licença de software para este sistema StorageGRID. Clique no link para ver os detalhes na página MANUTENÇÃO sistema Licença .

Informações relacionadas

- [Administrar o StorageGRID](#)
- [Configurar notificações por e-mail para alertas](#)

- [Utilize a monitorização SNMP](#)

Monitorar os estados de conexão do nó


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

O que você vai precisar

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



Sobre esta tarefa

Os nós podem ter um de três estados de conexão:

- **Não conectado - desconhecido** : o nó não está conectado à grade por um motivo desconhecido. Por exemplo, a conexão de rede entre nós foi perdida ou a energia está inativa. O alerta **não é possível se comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.



Um nó pode aparecer como desconhecido durante operações de desligamento gerenciado. Nesses casos, você pode ignorar o estado desconhecido.

- **Não conectado - 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.

Passos

1. Se um ícone azul ou cinza aparecer no painel Saúde do Painel, clique no ícone ou clique em **Detalhes da grade**. (Os ícones azul ou cinza e o link **Detalhes da grade** aparecem somente se pelo menos um nó estiver desconectado da grade.)

A página Visão geral do primeiro nó azul na árvore de nós é exibida. Se não houver nós azuis, a página Visão geral do primeiro nó cinza na árvore será exibida.

No exemplo, o nó de armazenamento chamado DC1-S3 tem um ícone azul. O **Estado da conexão** no painel informações do nó é **desconhecido** e o alerta **não é possível se comunicar com o nó** está ativo. O alerta indica que um ou mais serviços não respondem ou que o nó não pode ser alcançado.

The screenshot shows the StorageGRID Webconsole interface. On the left, a navigation pane lists nodes under two data centers (DC1 and DC2). DC2-ARC1 is highlighted with a blue icon. The main panel displays the details for DC2-ARC1 (Archive Node). The 'Node information' section shows the node's name, type, ID, software version, and IP addresses. The 'Connection state' is 'Unknown'. Below this, an 'Alerts' section contains a table with one alert: 'Unable to communicate with node'. The alert has a severity of 'Major', was triggered 9 days ago, and lists unresponsive services: 'arc, dynip, ssm'.

2. Se um nó tiver um ícone azul, siga estas etapas:

a. Selecione cada alerta na tabela e siga as ações recomendadas.

Por exemplo, talvez seja necessário reiniciar um serviço que tenha parado ou reiniciado o host para o nó.

b. Se você não conseguir colocar o nó novamente on-line, entre em Contato com o suporte técnico.

3. Se um nó tiver um ícone cinza, siga estas etapas:

Os nós cinzentos são esperados durante os procedimentos de manutenção e podem estar associados a um ou mais alertas. Com base na questão subjacente, esses nós "administrativamente para baixo" geralmente voltam online sem nenhuma intervenção.

a. Revise a seção Alertas e determine se algum alerta está afetando esse nó.

b. Se um ou mais alertas estiverem ativos, selecione cada alerta na tabela e siga as ações recomendadas.

c. Se você não conseguir colocar o nó novamente on-line, entre em Contato com o suporte técnico.

Informações relacionadas

[Referência de alertas](#)

[Recuperar e manter](#)

Ver alertas atuais

Quando um alerta é acionado, um ícone de alerta é exibido no Painel de instrumentos. Um ícone de alerta também é exibido para o nó na página nós. Uma notificação por e-mail também pode ser enviada, a menos que o alerta tenha sido silenciado.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Opcionalmente, você assistiu o vídeo: "[Vídeo: Visão geral dos alertas](#)".



Passos

1. Se um ou mais alertas estiverem ativos, execute um dos seguintes procedimentos:

- No painel Saúde do Painel, clique no ícone de alerta ou clique em **alertas atuais**. (Um ícone de alerta e o link **alertas atuais** aparecem somente se pelo menos um alerta estiver ativo.)
- Selecione **ALERTAS current**.

A página Alertas atuais é exibida. Ele lista todos os alertas que afetam o seu sistema StorageGRID atualmente.

Current Alerts [Learn more](#)

View the current alerts affecting your StorageGRID system.

Name	Severity	Time triggered	Site / Node	Status	Current values
Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job.	2 Major	9 minutes ago <i>(newest)</i> 19 minutes ago <i>(oldest)</i>		2 Active	
Low root disk capacity The space available on the root disk is low.	Minor	25 minutes ago	Data Center 1 / DC1-S1-99-51	Active	Disk space available: 2.00 GB Total disk space: 21.00 GB
Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire.	Major	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 14
Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire.	Minor	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 30
Low installed node memory The amount of installed memory on a node is low.	8 Critical	a day ago <i>(newest)</i> a day ago <i>(oldest)</i>		8 Active	




Por padrão, os alertas 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 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 Alertas atuais é atualizada a cada dois minutos.

2. Reveja as informações na tabela.

Cabeçalho da coluna	Descrição
Nome	O nome do alerta e sua descrição.
Gravidade	<p>A gravidade do alerta. Se vários alertas forem agrupados, a linha de título mostrará quantas instâncias desse alerta estão ocorrendo em 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.
Tempo acionado	Há quanto tempo o alerta foi acionado. 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>).
Local/nó	O nome do site e do nó onde o alerta está ocorrendo. Se vários alertas forem agrupados, os nomes do site e do nó não serão exibidos na linha de título.
Estado	Se o alerta está ativo ou foi silenciado. 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.
Valores atuais	<p>O valor atual 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 estiverem agrupados, os valores atuais não serão exibidos na linha de título.</p>

3. Para expandir e recolher grupos de alertas:

- Para mostrar os alertas individuais em um grupo, clique no cursor para baixo ▼ no cabeçalho ou clique no nome do grupo.
- Para ocultar os alertas individuais em um grupo, clique no cursor para cima ▲ no cabeçalho ou clique no nome do grupo.

							<input checked="" type="checkbox"/> Group alerts	Active ▼
Name	Severity	Time triggered	Site / Node	Status	Current values			
▲ <u>Low object data storage</u> The disk space available for storing object data is low.	▲ 5 Minor	a day ago (newest) a day ago (oldest)		5 Active				
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S2-233	Active	Disk space remaining: 525.17 GB Disk space used: 243.06 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC1 225-230 / DC1-S1-226	Active	Disk space remaining: 525.17 GB Disk space used: 325.65 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S3-234	Active	Disk space remaining: 525.17 GB Disk space used: 381.55 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC1 225-230 / DC1-S2-227	Active	Disk space remaining: 525.17 GB Disk space used: 282.19 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S1-232	Active	Disk space remaining: 525.17 GB Disk space used: 189.24 KB Disk space used (%): 0.000%			

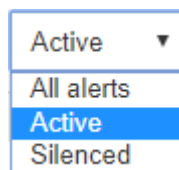
4. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **alertas de grupo** na parte superior da tabela.



5. Para classificar alertas ou grupos de alertas, clique nas 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 **Alerta de grupo** não está selecionado, 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.

6. Para filtrar os alertas por status, use o menu suspenso na parte superior da tabela.



- Selecione **todos os alertas** para visualizar todos os alertas atuais (alertas ativos e silenciados).
- Selecione **Ativo** para exibir somente os alertas atuais ativos.
- Selecione **silenciado** para visualizar apenas os alertas atuais que foram silenciados. [Silenciar notificações de alerta](#) Consulte .

7. Para ver detalhes de um alerta específico, selecione-o na tabela.

É apresentada uma caixa de diálogo para o alerta. [Veja um alerta específico](#) Consulte .

Exibir alertas resolvidos

Você pode pesquisar e exibir um histórico de alertas que foram resolvidos.

O que você vai precisar

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

Passos

1. Para exibir alertas resolvidos, siga um destes procedimentos:

- No painel Saúde do Painel, clique em **alertas resolvidos recentemente**.

O link **Recently resolved alerts** (alertas resolvidos recentemente) aparece apenas se um ou mais alertas tiverem sido acionados na semana passada e estiverem agora resolvidos.

- Selecione **ALERTAS resolvidos**. A página Alertas resolvidos é exibida. Por padrão, os alertas resolvidos que foram acionados na última semana são exibidos, com os alertas acionados mais recentemente exibidos primeiro. Os alertas nesta página foram exibidos anteriormente na página Alertas atuais ou em uma notificação por e-mail.

Resolved Alerts
Search and view alerts that have been resolved.




When triggered ^x Severity ^x Alert rule ^x Node ^x


Last week Filter by severity Filter by rule Filter by node Search

Name	Severity	Time triggered	Time resolved	Site / Node	Triggered values
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S2	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S3	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S4	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-ADM1	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-ADM2	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S1	Total RAM size: 8.37 GB

2. Reveja as informações na tabela.

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

Cabeçalho da coluna	Descrição
Gravidade	<p>A gravidade do alerta.</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.
Tempo acionado	Há quanto tempo o alerta foi acionado.
Tempo resolvido	Há quanto tempo o alerta foi resolvido.
Local/nó	O nome do site e do nó onde o alerta ocorreu.
Valores acionados	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.

3. Para classificar toda a lista de alertas resolvidos, clique nas setas para cima/para baixo  em cada cabeçalho de coluna.

Por exemplo, talvez você queira classificar os alertas resolvidos por **Site/nó** para ver os alertas que afetaram um nó específico.

4. Opcionalmente, filtre a lista de alertas resolvidos usando os menus suspensos na parte superior da tabela.

- a. Selecione um período de tempo no menu suspenso **When Triggered** para mostrar alertas resolvidos com base em quanto tempo atrás eles foram acionados.

Você pode pesquisar alertas que foram acionados nos seguintes períodos de tempo:

- Na última hora
- Último dia
- Semana passada (vista predefinida)
- No mês passado
- Qualquer período de tempo
- Personalizado (permite especificar a data de início e a data de fim para o período de tempo)

- b. Selecione uma ou mais severidades no menu suspenso **gravidade** para filtrar os alertas resolvidos de uma gravidade específica.

- c. 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.

- d. Selecione um ou mais nós no menu suspenso **Node** para filtrar os alertas resolvidos relacionados a um nó específico.

- e. Clique em **pesquisar**.

5. Para exibir detalhes de um alerta resolvido específico, selecione o alerta na tabela.

É apresentada uma caixa de diálogo para o alerta. [Veja um alerta específico](#) Consulte .

Veja um alerta específico

Você pode exibir informações detalhadas sobre um alerta que está afetando seu sistema StorageGRID ou um alerta que foi resolvido. Os detalhes incluem ações corretivas recomendadas, a hora em que o alerta foi acionado e o valor atual das métricas relacionadas a esse alerta.

Opcionalmente, você pode [silenciar um alerta atual](#) ou [atualize a regra de alerta](#).

O que você vai precisar

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

Passos

1. Siga um destes procedimentos, com base se você deseja exibir um alerta atual ou resolvido:

Cabeçalho da coluna	Descrição
Alerta atual	<ul style="list-style-type: none"> No painel Saúde no Painel, clique no link alertas atuais. Este link aparece somente se pelo menos um alerta estiver ativo no momento. Este link fica oculto se não houver alertas atuais ou se todos os alertas atuais tiverem sido silenciados. Selecione ALERTAS current. Na página NÓS, selecione a guia Visão geral para um nó que tenha um ícone de alerta. Em seguida, na seção Alertas, clique no nome do alerta.
Alerta resolvido	<ul style="list-style-type: none"> No painel Saúde do Painel, clique no link alertas resolvidos recentemente. (Este link aparece somente se um ou mais alertas foram acionados na semana passada e agora estão resolvidos. Este link fica oculto se nenhum alerta foi acionado e resolvido na última semana.) Selecione ALERTAS resolvidos.

2. Conforme necessário, expanda um grupo de alertas e selecione o alerta que deseja exibir.



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

<p>^ Low installed node memory The amount of installed memory on a node is low.</p>	<p>✖ 8 Critical</p>	<p>a day ago (newest) a day ago (oldest)</p>		<p>8 Active</p>	
<p><u>Low installed node memory</u> The amount of installed memory on a node is low.</p>	<p>✖ Critical</p>	<p>a day ago</p>	<p>Data Center 2 / DC2-S1-99-56</p>	<p>Active</p>	<p>Total RAM size: 8.38 GB</p>

Uma caixa de diálogo é exibida e fornece detalhes para o alerta selecionado.

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

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](#)

Time triggered

2019-07-15 17:07:41 MDT (2019-07-15 23:07:41 UTC)

Status
Active ([silence this alert](#))

Site / Node
Data Center 2 / DC2-S1-99-56




Severity
✖ Critical

Total RAM size
8.38 GB

Condition
[View conditions](#) | [Edit rule](#)

Close

3. Reveja os detalhes do alerta.

Informações	Descrição
<i>title</i>	O nome do alerta.
<i>primeiro parágrafo</i>	A descrição do alerta.
Ações recomendadas	As ações recomendadas para este alerta.
Tempo acionado	A data e a hora em que o alerta foi acionado na sua hora local e em UTC.
Tempo resolvido	Apenas para alertas resolvidos, a data e a hora em que o alerta foi resolvido na sua hora local e na UTC.
Estado	O estado do alerta: Ativo, silenciado ou resolvido.
Local/nó	O nome do site e do nó afetados pelo alerta.
Gravidade	<p>A gravidade do alerta.</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.
<i>valores de dados</i>	O valor atual da métrica para este alerta. 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 metadados baixo incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

4. Opcionalmente, clique em **Silenciar este alerta** para silenciar a regra de alerta que fez com que esse alerta fosse acionado.

Você deve ter a permissão Gerenciar Alertas ou acesso root 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.

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

a. A partir dos detalhes do alerta, clique em **Ver condições**.

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

The screenshot shows a pop-up window titled "Low installed node memory". It lists two conditions:

- Major** `node_memory_MemTotal_bytes < 24000000000`
- Critical** `node_memory_MemTotal_bytes < 12000000000`

On the right side of the pop-up, there is a "Condition" section with a "View conditions" link (underlined) and an "Edit rule" link with an external link icon. A mouse cursor is pointing at the "View conditions" link. Above the pop-up, the text "Total RAM size 8.38 GB" is visible.

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

6. Opcionalmente, clique em **Editar regra** para editar a regra de alerta que fez com que esse alerta fosse acionado:

Você deve ter a permissão Gerenciar Alertas ou 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.

7. Para fechar os detalhes do alerta, clique em **Fechar**.

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.

O que você vai precisar

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

Passos

1. Selecione **SUPORTE Alarmes (legacy) Alarmes atuais**.

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 aparece (**SUPPORT Tools Grid topology Grid Node Service Alarmes**).



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

- 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 \(sistema legado\)](#)

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

Você precisa monitorar 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 que você vai precisar

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

Sobre esta tarefa

O Painel no Gerenciador de Grade permite que você avalie rapidamente quanto armazenamento está disponível para toda a grade e para cada data center. A página nós fornece valores mais detalhados para

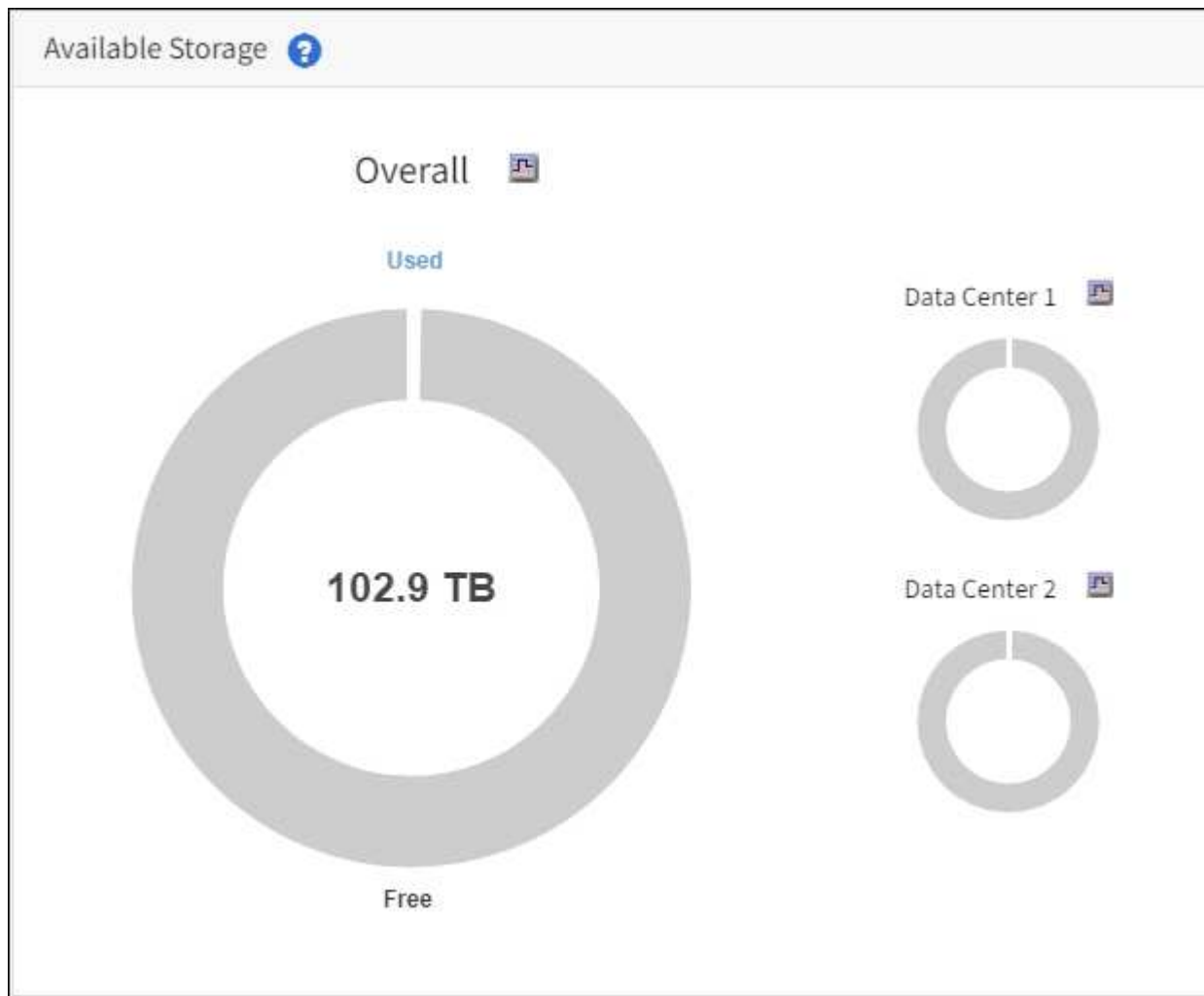
dados de objetos e metadados de objetos.

Passos

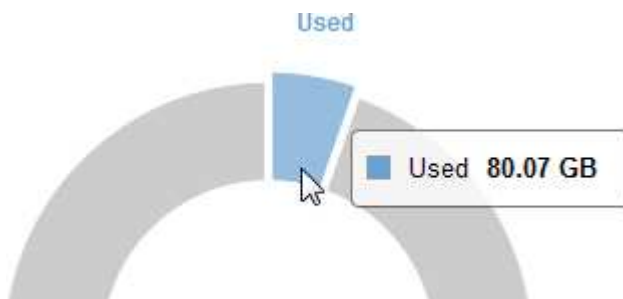
1. Avalie a quantidade de storage disponível para toda a grade e para cada data center.
 - a. Selecione **Painel**.
 - b. No painel armazenamento disponível, anote o resumo geral da capacidade de armazenamento livre e usada.




O resumo não inclui Mídia de arquivamento.



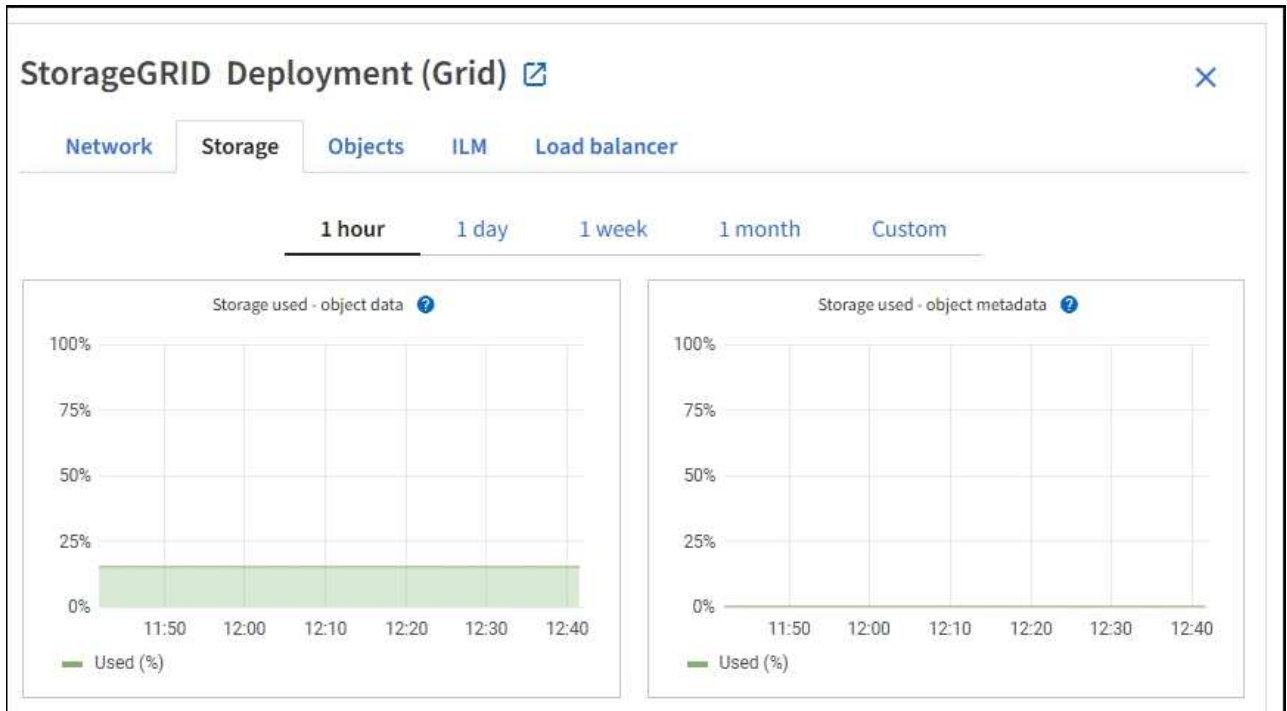
- a. Coloque o cursor sobre as seções de capacidade livre ou usada do gráfico para ver exatamente quanto espaço é livre ou usado.



- b. Para grades de vários locais, revise o gráfico de cada data center.
- c. Clique no ícone do gráfico  para o gráfico geral ou para um data center individual para exibir um gráfico que mostra o uso da capacidade ao longo do tempo.

Aparece um gráfico que mostra a porcentagem de capacidade de armazenamento utilizada (%) em comparação com o tempo.

2. Determine quanto storage foi usado e quanto storage permanece disponível para dados de objetos e metadados de objetos.
 - a. Selecione **NODES**.
 - b. Selecione **grid Storage**.



- c. Passe o cursor sobre os gráficos **Storage Used - Object data** e **Storage Used - Object metadata** para ver quanto armazenamento de objetos e metadados de objetos está disponível para toda a grade e quanto foi usado ao longo do tempo.



Os valores totais de um site ou da grade não incluem nós que não tenham métricas relatadas 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

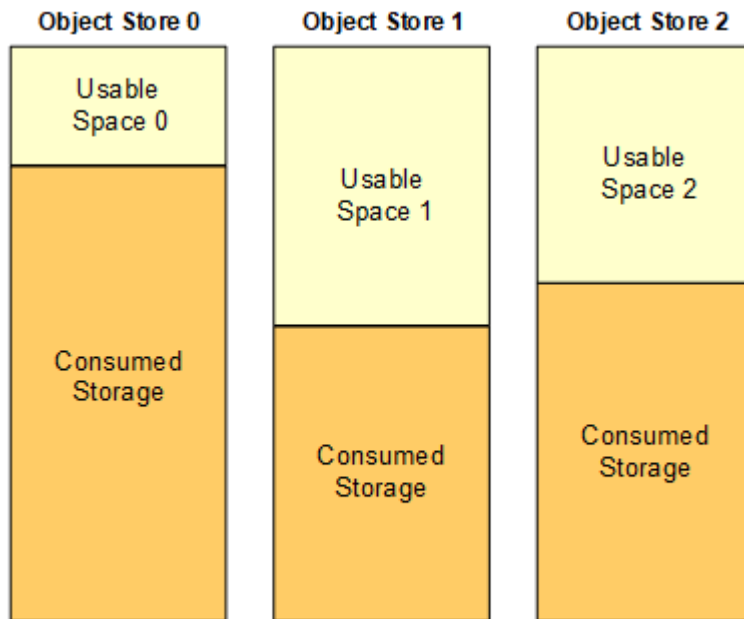
Monitore o espaço utilizável total para cada nó de storage para garantir que o nó tenha espaço suficiente para novos dados de objeto.

O que você vai precisar

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

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

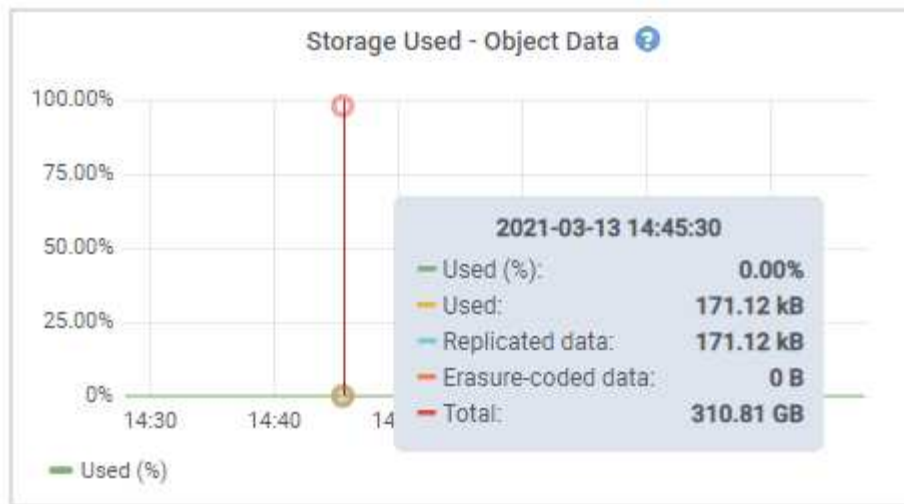
1. Selecione **NÓS Storage Node Storage**.

Os gráficos e tabelas para o nó aparecem.

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

São apresentados os seguintes valores:

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



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



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

Disk devices

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

Volumes

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

Object stores

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

4. Monitore os valores ao longo do tempo para estimar a taxa na qual o espaço de armazenamento utilizável está sendo consumido.
5. Para manter as operações normais do sistema, adicione nós de storage, adicione volumes de storage ou 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.

Armazenamento de dados de objetos baixo 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.

O que você vai precisar

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

Sobre esta tarefa

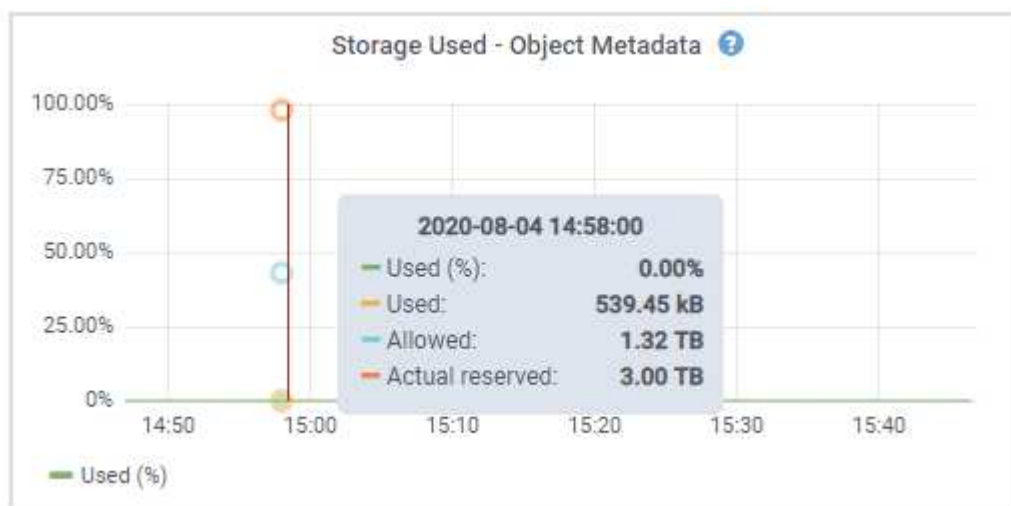
O StorageGRID mantém três cópias de metadados de objetos em cada local para fornecer redundância e proteger os metadados de objetos da perda. As três cópias são distribuídas uniformemente por todos os nós de storage em cada local, usando o espaço reservado para metadados no volume de storage 0 de cada 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. Passe o cursor sobre o gráfico armazenamento usado - metadados de objetos para ver os valores de um tempo específico.



Valor	Descrição	Métrica Prometheus
Usado (%)	A porcentagem do espaço de metadados permitido que foi usado neste nó de storage.	<code>storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes</code>
Usado	Os bytes do espaço de metadados permitido que foram usados neste nó de armazenamento.	<code>storagegrid_storage_utilization_metadata_bytes</code>
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 Instruções para administrar o StorageGRID .	<code>storagegrid_storage_utilization_metadata_allowed_bytes</code>
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 Instruções para administrar o StorageGRID .	<i>Metric será adicionado em uma versão futura.</i>



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 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.

O que você vai precisar


Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

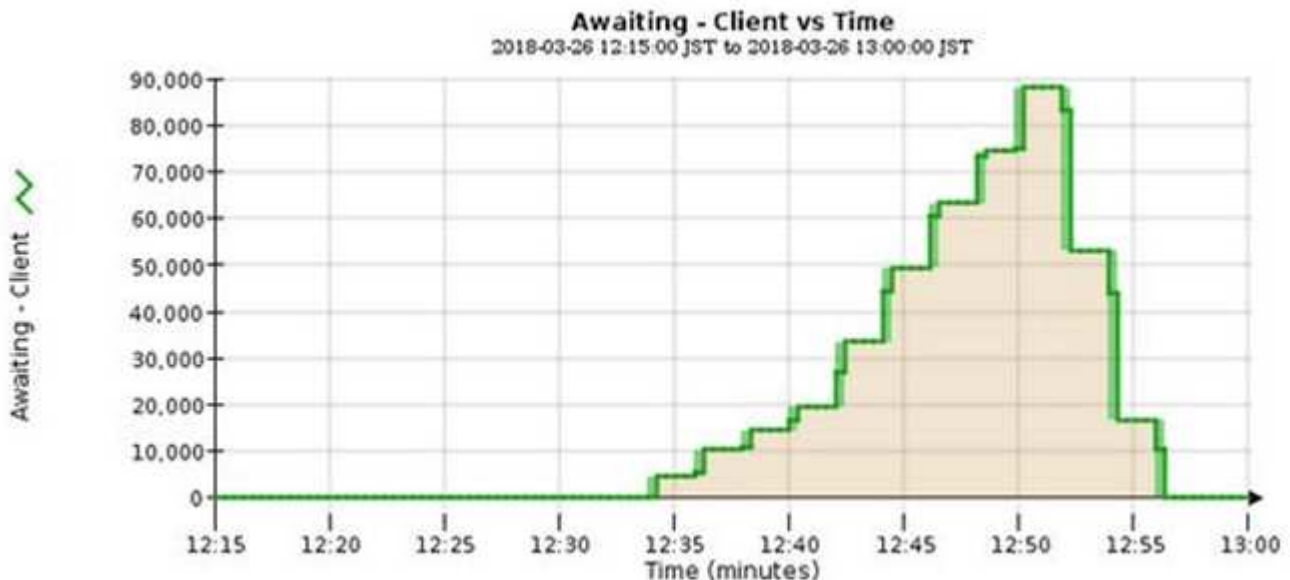
O sistema StorageGRID gerencia objetos aplicando a política ILM ativa. A política ILM e as regras ILM associadas determinam quantas cópias são feitas, o tipo de cópias que são criadas, onde as cópias são colocadas e o tempo de retenção de cada cópia.

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 pode monitorar se o StorageGRID está acompanhando as ações do cliente traçando o atributo awaiting - Client.

Para traçar este atributo:

1. Faça login no Gerenciador de Grade.
2. No Painel, localize a entrada **aguardando - Cliente** no painel Gerenciamento do ciclo de vida da Informação (ILM).
3. Clique no ícone do gráfico .

O gráfico de exemplo mostra uma situação em que o número de objetos que aguardam a avaliação do ILM aumentou temporariamente de forma insustentável, depois diminuiu eventualmente. Tal tendência indica que o ILM não foi temporariamente cumprido em tempo quase real.



Picos temporários no gráfico de aguardando - o cliente deve ser esperado. Mas se o valor mostrado no gráfico continuar a aumentar e nunca declinar, a grade requer 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.

Você pode investigar mais filas de ILM usando a página **NODES**.

Passos

1. Selecione **NODES**.
2. Selecione **grid name ILM**.
3. Passe o cursor sobre o gráfico ILM Queue 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 conexões de rede e desempenho

Os nós de grade devem ser capazes de se comunicar uns com os outros para permitir que a grade opere. A integridade da rede entre nós e locais, e a largura de banda da rede entre locais, são essenciais para operações eficientes.

O que você vai precisar

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

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 simplesmente a baixo desempenho de ingestão e backlogs de ILM.

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

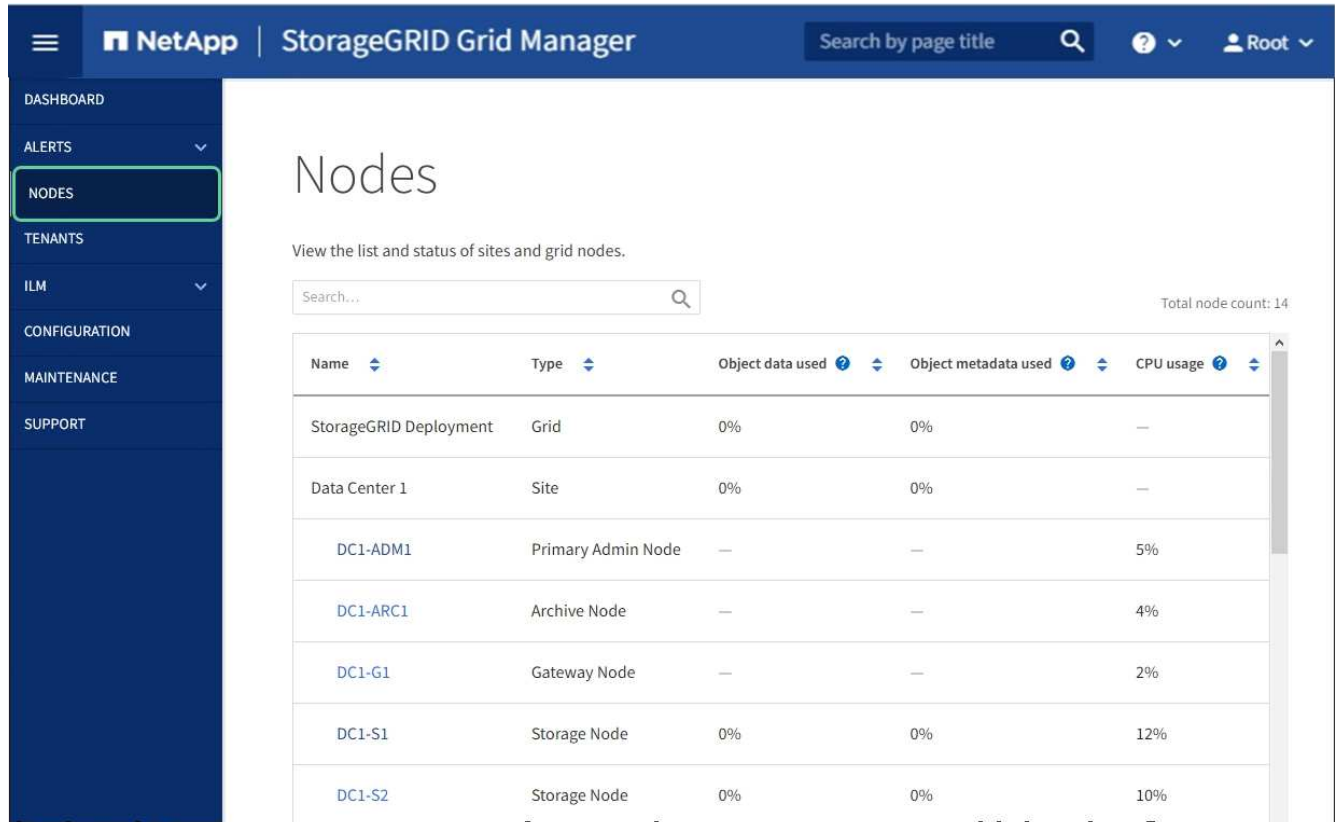
Além disso, considere criar políticas de classificação de tráfego de rede para fornecer monitoramento e

limitação para o tráfego relacionado a locatários específicos, buckets, sub-redes ou pontos de extremidade do balanceador de carga. Consulte [Instruções para administrar o StorageGRID](#).

Passos

1. Selecione **NODES**.

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

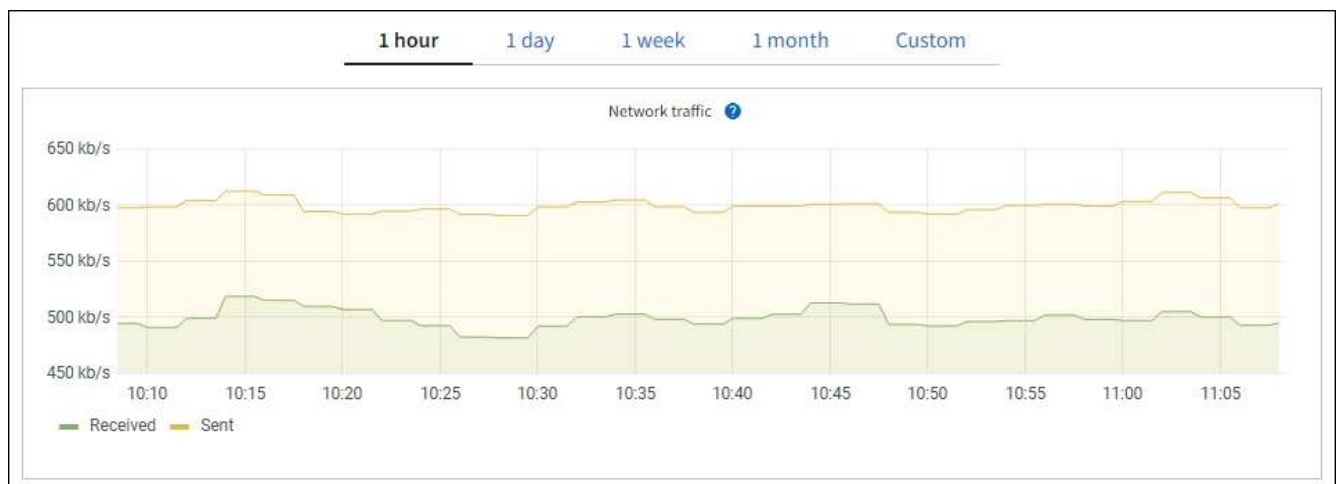


The screenshot shows the NetApp StorageGRID Grid Manager interface. The left sidebar has a menu with 'NODES' highlighted. The main content area is titled 'Nodes' and contains a search bar and a table of nodes. The table has the following data:

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	—	—	5%
DC1-ARC1	Archive Node	—	—	4%
DC1-G1	Gateway Node	—	—	2%
DC1-S1	Storage Node	0%	0%	12%
DC1-S2	Storage Node	0%	0%	10%

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.

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.

+ Create Edit Remove Metrics		
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.

b. 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**.

c. 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.

Para criar, editar ou excluir políticas de classificação de tráfego, consulte [Instruções para administrar o StorageGRID](#).

Informações relacionadas

[Veja a guia rede](#)

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

Monitore os recursos no nível do nó

Você deve monitorar nós de grade individuais para verificar seus níveis de utilização de recursos.

O que você vai precisar

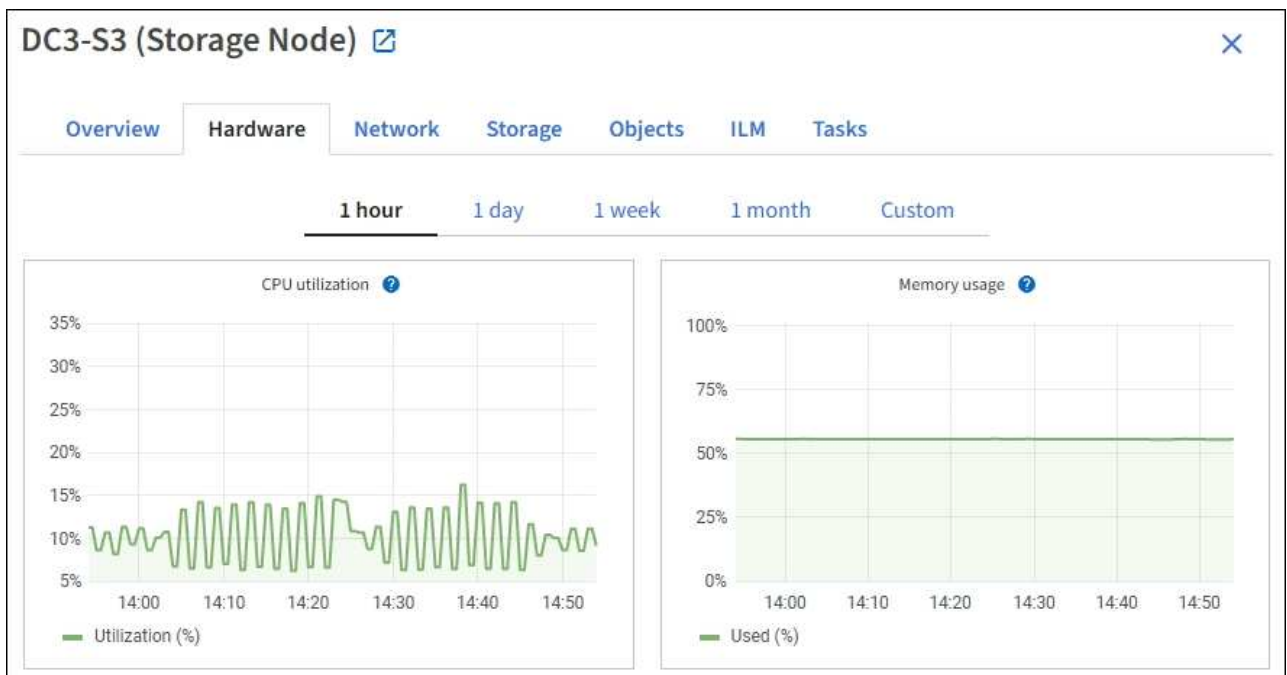
- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

Se os nós estiverem sobrecarregados consistentemente, mais nós poderão ser necessários para operações eficientes.

Passos

1. Para exibir informações sobre a utilização de hardware de um nó de grade:
 - a. Na página **NÓS**, selecione o nó.
 - b. Selecione a guia **hardware** para exibir gráficos de utilização da CPU e uso da memória.



- c. 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.

- d. 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 status de todos os componentes deve ser "nominal". Investigue componentes que tenham qualquer outro status.

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 do cliente estão associadas a uma conta de locatário. Você pode usar o Gerenciador de Grade para monitorar o uso de storage ou o tráfego de rede de um locatário ou usar o log de auditoria ou os painéis do Grafana para coletar informações mais detalhadas sobre como os locatários estão usando o StorageGRID.

O que você vai precisar

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



Sobre esta tarefa

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

Passos

1. Selecione **TENANTS** para analisar a quantidade de armazenamento usada por todos os inquilinos.

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 de utilização da cota e quota contêm um traço (nº 8212;).

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 style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

Você pode fazer login em uma conta de locatário selecionando o link de login → na coluna **entrar/Copiar URL** da tabela.

Você pode copiar o URL da página de login de um locatário selecionando o link URL de cópia na coluna **Sign in/Copy URL** da tabela.

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

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

O conteúdo de um arquivo .csv 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 arquivo .csv em um aplicativo de Planilha ou usá-lo em automação.

3. Para exibir detalhes de um locatário específico, incluindo gráficos de uso, selecione o nome da conta do locatário na página de locatários.

Tenant 02

Tenant ID: 4103 1879 2208 5551 2180 [📄](#) Quota utilization: 85%

Protocol: S3 Logical space used: 85.00 GB

Object count: 500 Quota: 100.00 GB

[Sign in](#) [Edit](#) [Actions](#) ▾

[Space breakdown](#) [Allowed features](#)

Bucket space consumption

85.00 GB of 100.00 GB used

15.00 GB remaining (15%).

0 25% 50% 75% 100%

● bucket-01 ● bucket-02 ● bucket-03

Bucket details

[Export to CSV](#) [🔍](#) Displaying 3 results

Name	Region	Space used	Object count
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

- **Visão geral do locatário**

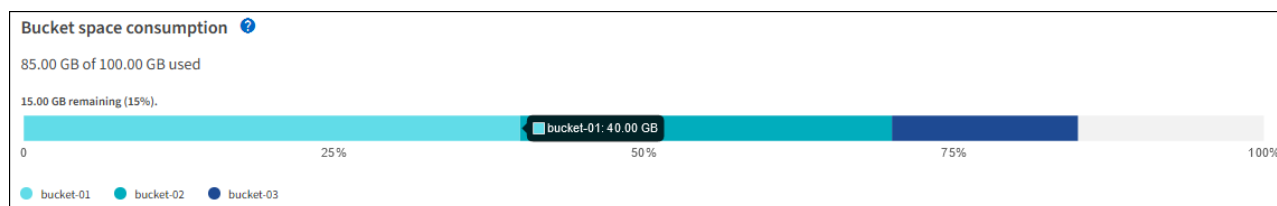
A área de visão geral do locatário contém valores para contagem de objetos, utilização de cotas, espaço lógico usado e configuração de cota.

- * Espaço de quebra — consumo de espaço*

A guia repartição de espaço inclui valores para o consumo total de espaço do bucket (S3) ou container (Swift), bem como espaço usado e contagem de objetos para cada bucket ou contentor.

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 o alerta **Alto uso da cota do locatário** 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 mais informações, consulte a referência de alertas.

- * Espaço de quebra — Detalhes do balde ou do recipiente*

A tabela **Bucket details** (S3) ou **Container details** (Swift) lista os buckets ou contentores 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.

4. 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 .csv de um locatário S3 individual se parece com o seguinte exemplo:

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

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

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

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.



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-7665bdc894b

Displaying 2 traffic classification policies.

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

Para criar, editar ou excluir políticas de classificação de tráfego, consulte as instruções de administração do StorageGRID.

6. Opcionalmente, use 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 as instruções para entender as mensagens de auditoria para obter mais informações.

7. 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.

Informações relacionadas

[Referência de alertas](#)

[Rever registros de auditoria](#)

[Administrar o StorageGRID](#)

[Analisar as métricas de suporte](#)

Monitorar a capacidade de arquivamento

Não é possível monitorar diretamente a capacidade de um sistema de storage 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.

O que você vai precisar

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

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.

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.

O que você vai precisar

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

Sobre esta tarefa

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



O serviço CLB está obsoleto.

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.

Consulte a seção sobre como configurar conexões de cliente nas instruções de administração do StorageGRID.

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 Mestre.

Os nós com a função de Mestre 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 a guia **Load Balancer**.
 - 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 exibir uma discriminação mais detalhada do tráfego que está sendo servido pelo serviço Load Balancer.
2. Se os clientes S3 ou Swift se conectarem usando o serviço CLB (obsoleto), execute as seguintes verificações:

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

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

- d. Para cada nó de gateway que deve estar distribuindo ativamente solicitações de cliente, selecione **SUPPORT Tools Grid topology**.
 - e. Selecione **Gateway Node CLB HTTP Overview Main**.
 - f. Revise o número de **sessões de entrada - estabelecidas** para verificar se o Gateway Node tem lidado ativamente com solicitações.
3. 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.

Informações relacionadas

Aplique hotfixes ou atualize o software, se necessário

Se estiver disponível uma correção ou uma nova versão do software StorageGRID, deve avaliar se a atualização é adequada ao seu sistema e instalá-la, se necessário.

Sobre esta tarefa

Os hotfixes do StorageGRID contêm alterações de software que são disponibilizadas fora de uma versão de recurso ou patch. As mesmas alterações estão incluídas em uma versão futura.

Passos

1. Vá para a página de downloads do NetApp para StorageGRID.

["NetApp Downloads: StorageGRID"](#)

2. Selecione a seta para baixo para o campo **Type/Select Version** (tipo/Selecionar versão) para ver uma lista das atualizações disponíveis para download:

- **Versões de software StorageGRID:** 11.x.y
- **StorageGRID hotfixes:** 11.x.y.z

3. Reveja as alterações incluídas na atualização:

- a. Selecione a versão no menu suspenso e clique em **Go**.
- b. Inicie sessão utilizando o nome de utilizador e a palavra-passe da sua conta NetApp.
- c. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.

É apresentada a página de transferências para a versão selecionada.

4. Saiba mais sobre as alterações incluídas na versão de software ou hotfix.

- Para uma nova versão de software, consulte o tópico "Novidades" nas instruções para atualizar o StorageGRID.
- Para obter um hotfix, baixe o arquivo README para obter um resumo das alterações incluídas no hotfix.

5. Se decidir que é necessária uma atualização de software, localize as instruções antes de prosseguir.

- Para uma nova versão de software, siga cuidadosamente as instruções para atualizar o StorageGRID.
- Para obter um hotfix, localize o procedimento de hotfix nas instruções de recuperação e manutenção

Informações relacionadas

[Atualizar o software](#)

[Recuperar e manter](#)

Gerencie 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 exibido no Painel no 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**.
- 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

Há uma série de semelhanças entre o sistema de alerta e o sistema de alarme legado, 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 (alertas atuais) no Painel de instrumentos. • Selecione o alerta na página NÓS Visão geral. • Selecione ALERTAS current. <p>Ver alertas atuais</p>	<p>Selecione SUORTE Alarmes (legacy) Alarmes atuais.</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 resolvidos.</p> <p>Exibir alertas resolvidos</p>	<p>Selecione SUORTE Alarmes (legado) 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 reconhecer alarmes para reconhecer alarmes. Você deve ter as permissões Configuração da Página de topologia de Grade e outras permissões de Configuração de Grade para gerenciar alarmes globais e notificações por 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>	<p>Selecione CONFIGURATION Monitoring SNMP Agent.</p> <p>Utilize a monitorização SNMP</p> <p>Nota: As notificações SNMP não são enviadas para cada alarme ou gravidade do alarme.</p> <p>Alarmes que geram notificações SNMP (sistema legado)</p>

	Alertas	Alarmes (sistema legado)
Como posso controlar quem recebe notificações?	<ol style="list-style-type: none"> 1. Selecione ALERTAS Configuração do e-mail. 2. Na seção destinatários, insira um endereço de e-mail para cada lista de e-mail ou pessoa que deve receber um e-mail quando ocorrer um alerta. <p>Configurar notificações por e-mail para alertas</p>	<ol style="list-style-type: none"> 1. Selecione SUPPORT Alarmes (legacy) Configuração de e-mail legado. 2. Criando uma lista de discussão. 3. Selecione notificações. 4. Selecione a lista de discussão. <p>Gerenciar alarmes (sistema legado)</p>
Quais nós de administrador enviam notificações?	<p>Um único nó Admin (o "remetente preferido").</p> <p>Administrar o StorageGRID</p>	<p>Um único nó Admin (o "remetente preferido").</p> <p>Administrar o StorageGRID</p>
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>	<ol style="list-style-type: none"> 1. Selecione CONFIGURATION > System > Display OPTIONS. 2. Marque a caixa de seleção notificação suprimir tudo. <p>Nota: A supressão de notificações por e-mail em todo o sistema também suprime os e-mails do AutoSupport acionados por eventos.</p> <p>Gerenciar alarmes (sistema legado)</p>

	Alertas	Alarmes (sistema legado)
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 SUORTE Alarmes (legado) 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>
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 SUORTE Alarmes (legado) 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

Os alertas permitem-lhe monitorizar vários eventos e condições no seu sistema StorageGRID. Você pode gerenciar alertas criando alertas personalizados, editando ou desativando os alertas padrão, configurando notificações de e-mail para alertas e silenciando notificações de alerta.

Sobre os alertas do StorageGRID

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

- O sistema de alerta se concentra em problemas acionáveis no sistema. Os alertas são acionados para eventos que exigem sua atenção imediata, não para eventos que podem ser ignorados com segurança.
- A página Alertas atuais fornece uma interface amigável para visualizar problemas atuais. Você pode classificar a lista por alertas individuais e grupos de alertas. Por exemplo, talvez você queira classificar todos os alertas por nó/site para ver quais alertas estão afetando um nó específico. Ou, talvez você queira classificar os alertas em um grupo por tempo acionado para encontrar a instância mais recente de um alerta específico.
- A página Alertas resolvidos fornece informações semelhantes às da página Alertas atuais, mas permite pesquisar e visualizar um histórico dos alertas que foram resolvidos, incluindo quando o alerta foi acionado e quando foi resolvido.
- Vários alertas do mesmo tipo são agrupados em um e-mail para reduzir o número de notificações. Além disso, vários alertas do mesmo tipo são exibidos como um grupo na página Alertas. Você pode expandir e

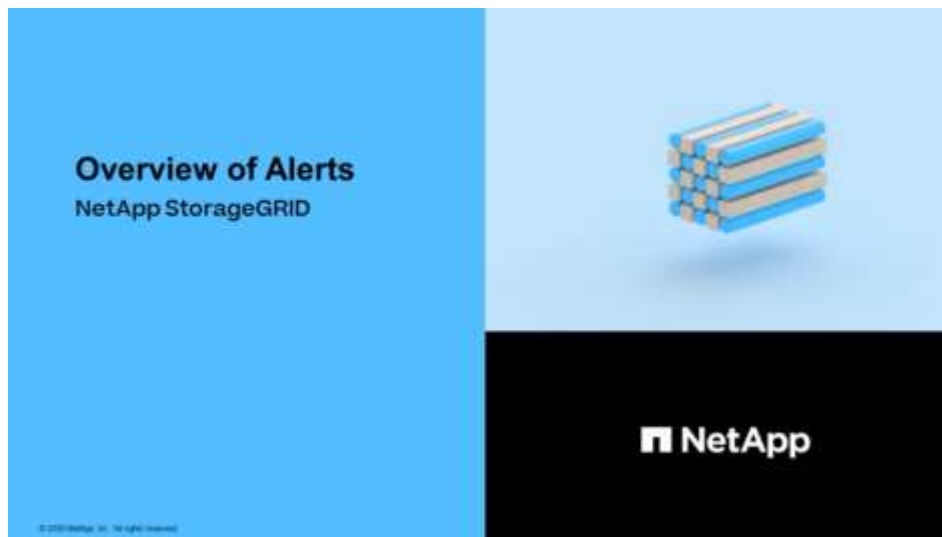
recolher grupos de alerta para mostrar ou ocultar os alertas individuais. Por exemplo, se vários nós relatarem o alerta **não é possível se comunicar com o nó** aproximadamente ao mesmo tempo, somente um email é enviado e o alerta é mostrado como um grupo na página Alertas.

- Os alertas usam nomes e descrições intuitivas para ajudá-lo a entender rapidamente o problema. As notificações de alerta incluem detalhes sobre o nó e o site afetado, a gravidade do alerta, o tempo em que a regra de alerta foi acionada e o valor atual das métricas relacionadas ao alerta.
- As notificações de e-mails de alerta e as listagens de alerta nas páginas Alertas atuais e alertas resolvidos fornecem ações recomendadas para resolver um alerta. Essas ações recomendadas geralmente incluem links diretos para o centro de documentação do StorageGRID para facilitar a localização e o acesso a procedimentos de solução de problemas mais detalhados.
- Se você precisar suprimir temporariamente as notificações de um alerta em um ou mais níveis de gravidade, poderá silenciar facilmente uma regra de alerta específica por uma duração especificada e para toda a grade, um único local ou um único nó. Você também pode silenciar todas as regras de alerta, por exemplo, durante um procedimento de manutenção planejado, como uma atualização de software.
- Você pode editar as regras de alerta padrão conforme necessário. Você pode desativar completamente uma regra de alerta ou alterar suas condições de ativação e duração.
- Você pode criar regras de alerta personalizadas para direcionar as condições específicas que são relevantes para a sua situação e para fornecer suas próprias ações recomendadas. Para definir as condições para um alerta personalizado, você cria expressões usando as métricas Prometheus disponíveis na seção métricas da API de Gerenciamento de Grade.

Saiba mais

Para saber mais, reveja estes vídeos:

- ["Vídeo: Visão geral dos alertas"](#)



- ["Vídeo: Usando métricas para criar alertas personalizados"](#)

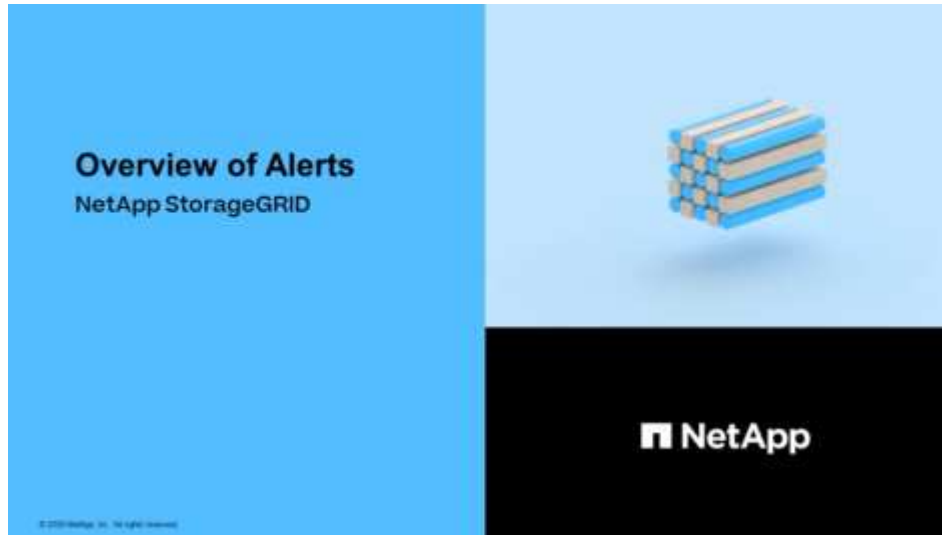
Ver regras de alerta

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.

O que você vai precisar

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



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.

+ Create custom rule Edit rule Remove custom rule			
Name	Conditions	Type	Status
<input type="radio"/> Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	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.
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	Se esta regra de alerta está atualmente ativada ou desativada. As condições para regras de alerta desativadas não são avaliadas, portanto, nenhum alerta é acionado.

Crie regras de alerta personalizadas

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

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#)
- Você tem a permissão Gerenciar Alertas ou acesso root
- Você está familiarizado com o [Métricas de Prometheus comumente usadas](#)
- Você entende "[Sintaxe das consultas Prometheus](#)"
- Opcionalmente, você assistiu ao vídeo: "[Vídeo: Usando métricas para criar alertas personalizados](#)"

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 "de sucesso" pode simplesmente 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

5

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.

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


Uma expressão básica é geralmente da forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

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

O padrão é 5 minutos.

7. Selecione **Guardar**.

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

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.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou 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

Description

Recommended Actions (optional) VMware installation- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)
"/>

Conditions ?

Minor

Major

Critical

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

Duration

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

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



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



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

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



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

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

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou acesso root.

Sobre esta tarefa

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



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

Passos

1. Selecione **ALERTAS regras**.

A página regras de alerta é exibida.

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

A caixa de diálogo Editar regra é exibida.

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

no momento.

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



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

5. Selecione **Guardar**.

Disabled aparece na coluna **Status**.

Remover regras de alerta personalizadas

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

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou 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 .

As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o remetente preferido. Por padrão, o nó de administração principal é selecionado. Consulte [Instruções para administrar o StorageGRID](#).



Notificações de intercetção e informação também são enviadas quando certos alarmes (sistema legado) são acionados em níveis de gravidade especificados ou superiores; no entanto, as notificações SNMP não são enviadas para cada alarme ou para cada gravidade de alarme. [Alarmes que geram notificações SNMP \(sistema legado\)](#)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.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou 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 mensagens AutoSupport. No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações.

Se sua implantação do StorageGRID incluir vários nós de administração, você poderá selecionar qual nó de administração deve ser o remetente preferido das notificações de alerta. O mesmo ""remetente preferido"" também é usado para notificações de alarme e mensagens AutoSupport. Por padrão, o nó de administração principal é selecionado. Para obter detalhes, consulte [Instruções para administrar o StorageGRID](#).

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 **Enviar certificado de cliente** 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-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMNopQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Send Client Certificate 

Client Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMNopQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Private Key 

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxy  
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 notificações de alarme e mensagens AutoSupport, 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.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou 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.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Gerenciar Alertas ou 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
<i>No results found.</i>				

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 grelha, o silêncio aplica-se a todos os locais e a todos os nós. Se selecionar um local, o silêncio aplica-se apenas aos nós nesse local.</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	<ol style="list-style-type: none"> a. Selecione ALERTAS silêncios. b. Na tabela, selecione o botão de opção para o silêncio que deseja editar. c. Selecione Editar. d. Altere a descrição, a quantidade de tempo restante, as severidades selecionadas ou o nó afetado. e. Selecione Guardar.

Opção	Descrição
Remova um silêncio	<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](#)

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 predefinidos 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.

Ícone	Cor	Gravidade do alarme	Significado
	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

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

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

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

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

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

Alarmes da mesma gravidade

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

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



Global Alarms

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

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<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 (50000000).



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	under10i	<=	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 de 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, não é possível desativar um único alarme em uma linha da 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.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter a permissão 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 (uma vez que 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 **SUPORTE Alarmes (legacy) Alarmes atuais**.

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

2. Selecione o nome do serviço na tabela.

A guia Alarmes para o serviço selecionado aparece (**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"/>



3. Marque a caixa de seleção **confirmar** para o alarme e clique em **aplicar alterações**.

O alarme não aparece mais no Painel de instrumentos 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 Dashboard de outro nó Admin, poderá continuar a ver o alarme ativo.

4. Conforme necessário, visualize os alarmes reconhecidos.

- a. Selecione **SUPORTE Alarmes (legacy) Alarmes atuais**.
- 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 Records Per Page Previous « 1 » Next

Exibir alarmes padrão (sistema legado)

Pode ver a lista de todos os alarmes herdados predefinidos.


O que você vai precisar

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



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 **SUPORTE Alarmes (legado) 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 Attribute Code 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"/>		XCVF (% 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.

O que você vai precisar

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



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 **SUPORTE Alarmes (legado) 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.

O que você vai precisar

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





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 muito 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 **SUPORTE Alarmes (legado) 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 equals

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.

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

Rumo	Descrição
Ativado	Selecione ou desmarque a caixa de seleção 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. • menos de • maior 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 e solte 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 antigo 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.

O que você vai precisar

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

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 **SUPORTE Alarmes (legado) 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.

O que você vai precisar

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

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 **SUPORTE Alarmes (legado) 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.

O que você vai precisar

- 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-mail.

O que você vai precisar

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

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 mensagens 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 mensagens 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 Credentials	Username: <input type="text" value="root"/> 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.

O que você vai precisar



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

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 Records Per Page





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.



O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter permissões de acesso específicas.
- 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: 2018-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  

Show Records Per Page





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 e-mail 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.

O que você vai precisar



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

O que você vai precisar


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

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.

Suprimir notificações de e-mail em todo o sistema

Você pode bloquear a capacidade do sistema StorageGRID de enviar notificações por e-mail para alarmes legados e mensagens AutoSupport acionadas por eventos.

O que você vai precisar

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

Sobre esta tarefa

Use esta opção para suprimir notificações de e-mail para alarmes legados e mensagens AutoSupport acionadas por eventos.



Esta opção não suprime as notificações por e-mail de alerta. Ele também não suprime mensagens AutoSupport semanais ou acionadas pelo usuário.

Passos

1. Selecione **CONFIGURATION System settings Display options**.
2. No menu Opções de exibição, selecione **Opções**.
3. Selecione **notificação suprimir tudo**.



Display Options

Updated: 2017-03-23 18:03:48 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input checked="" type="checkbox"/>

Apply Changes

4. Clique em **aplicar alterações**.

A página notificações (**Configuração notificações**) exibe a seguinte mensagem:



Notifications

Updated: 2016-03-17 14:06:48 PDT

All e-mail notifications are now suppressed.

Notifications (0 - 0 of 0)

	Suppress	Severity Levels				Service States		
E-mail List	<input checked="" type="checkbox"/>	Notice	Minor	Major	Critical	Unknown	Administratively Down	Actions
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Show Records Per Page

« »

Apply Changes

Configurar mensagens de auditoria e destinos de log

Mensagens de auditoria e logs registram atividades do sistema e eventos de segurança, e são ferramentas essenciais para monitoramento e solução de problemas. Você pode ajustar os níveis de auditoria para aumentar ou diminuir o tipo e o número de mensagens de auditoria registradas. Opcionalmente, você pode definir qualquer cabeçalho de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação de cliente. Você também pode configurar um servidor syslog externo e alterar o destino das informações de auditoria.

Para obter mais informações sobre mensagens de auditoria, [Rever registros de auditoria](#) consulte .

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de Manutenção ou Acesso root.

Sobre esta tarefa

Todos os nós do StorageGRID geram mensagens de auditoria e logs para rastrear a atividade e os eventos do sistema. Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode ajustar os níveis de auditoria para aumentar ou diminuir o tipo e o número de mensagens de auditoria registradas no log de auditoria. Opcionalmente, você pode configurar informações de auditoria para serem enviadas para um servidor syslog remoto ou para serem armazenadas temporariamente nos nós de origem para coleta manual.

Alterar os níveis de mensagens de auditoria no log 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	Descrição
Sistema	Por padrão, esse nível é definido como normal. Mensagens de auditoria do sistema Consulte .
Armazenamento	Por padrão, esse nível é definido como erro. Mensagens de auditoria de armazenamento de objetos Consulte .
Gerenciamento	Por padrão, esse nível é definido como normal. Mensagem de auditoria de gerenciamento Consulte .
O cliente lê	Por padrão, esse nível é definido como normal. O cliente lê mensagens de auditoria Consulte .
O cliente escreve	Por padrão, esse nível é definido como normal. O cliente escreve mensagens de auditoria Consulte .



Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10,3 ou posterior. Se você atualizou de 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**.

Audit and syslog server

Audit messages and logs record system activities and security events and are an essential tool for monitoring and troubleshooting.

Audit levels

Adjust audit levels to increase or decrease the type and number of audit messages recorded.

System	Normal
Storage	Error
Management	Normal
Client reads	Normal
Client writes	Normal

Audit protocol headers

Optionally, define any HTTP request headers you want to include in client read and write audit messages.

Header name 1

[Add another header](#)

Use external syslog server

By default, audit messages are saved on Admin Nodes and logs are saved on the nodes where they were generated. If you want to save audit messages and a subset of logs externally, configure an external syslog server.

i If you want to use an external syslog server, you must configure it first.

[Configure external syslog server](#)

If you want to change these log locations, select a different option below.

Log type	Log location
Audit log	Admin Nodes
Security events	Local nodes
Application logs	Local nodes

- Default (Admin Nodes/local nodes)
- External syslog server
- Admin Nodes and external syslog server
- Local nodes only

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.

Nível de auditoria	Descrição
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.
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.

3. Opcionalmente, em **cabeçalhos de protocolo de auditoria**, defina quaisquer cabeçalhos de solicitação HTTP que você deseja incluir em mensagens de auditoria de leitura e gravação de cliente. Use um asterisco (*) **como curinga para corresponder a zero ou mais caracteres. Use a sequência de escape (\)** para corresponder a um asterisco literal.



Os cabeçalhos de protocolo de auditoria aplicam-se apenas às solicitações S3 e Swift.

4. 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**.

5. Selecione **Guardar**

É apresentado um banner verde indicando que a sua configuração foi guardada com sucesso.

Use um servidor syslog externo

Você pode configurar um servidor syslog externo se quiser salvar informações de auditoria remotamente.

- Se você quiser salvar informações de auditoria em um servidor syslog externo, vá para [Configurar um servidor syslog externo](#).
- Se você não estiver usando um servidor syslog externo, vá para [Selecione destinos de informações de auditoria](#).

Selecione destinos de informações de auditoria

Você pode especificar onde os logs de auditoria, os logs de eventos de segurança e os logs de aplicativos são enviados.



Alguns destinos só estão disponíveis se você estiver usando um servidor syslog externo. [Consulte para configurar um servidor syslog externo](#)



Para obter mais informações sobre os logs do software StorageGRID, [Registos do software StorageGRID](#) consulte .

1. Na página servidor de auditoria e syslog, selecione o destino das informações de auditoria nas opções listadas:

Opção	Descrição
Padrão (nós de administração/nós locais)	As mensagens de auditoria são enviadas para o log de auditoria (<code>audit.log</code>) no Admin Node, e os logs de eventos de segurança e de aplicativos são armazenados nos nós em que foram gerados (também chamados de "o nó local").
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas no nó local. 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.
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (<code>audit.log</code>) no nó Admin e as informações de auditoria são enviadas para o servidor syslog externo e salvas no nó local. 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.
Somente nós locais	Nenhuma informação de auditoria é enviada para um Admin Node ou servidor syslog remoto. As informações de auditoria são salvas apenas nos nós que as geraram. Nota: O StorageGRID remove periodicamente esses 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.



As informações de auditoria geradas em cada nó local são armazenadas no `/var/local/log/localaudit.log`

1. Selecione **Guardar**.

É apresentada uma mensagem de aviso:



Alterar o destino do registo?

1. Confirme se deseja alterar o destino para informações de auditoria selecionando **OK**.

Um banner verde é exibido notificando que sua configuração de auditoria foi salva com êxito.

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

Informações relacionadas

[Considerações para servidor syslog externo](#)

[Administrar o StorageGRID](#)

[Solucionar problemas do servidor syslog externo](#)

Use um servidor syslog externo

Considerações para servidor syslog externo

Use as diretrizes a seguir para estimar o tamanho do servidor syslog externo de que você precisa.

O que é 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 configurar os destinos das informações de auditoria para que você possa reduzir o tráfego de rede em seus nós de administração e gerenciar as informações com mais eficiência. 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

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	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets 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: Taxa de operações de 8 x S3
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 são 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	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets 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 receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Para obter mais informações sobre como configurar os níveis de mensagens de auditoria e um servidor syslog externo, consulte o seguinte:

- [Configurar um servidor syslog externo](#)
- [Configurar mensagens de auditoria e destinos de log](#)

Configurar um servidor syslog externo

Se você quiser salvar logs de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora da grade, use este procedimento para configurar um servidor syslog externo.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de Manutenção ou Acesso root.
- Você tem um servidor syslog com a capacidade de receber e armazenar os arquivos de log. Para obter

mais informações, [Considerações para servidor syslog externo](#) consulte .

- Você tem as certificações de servidor e cliente corretas se planeja usar TLS ou RELP/TLS.

Sobre esta tarefa

Se você quiser enviar informações de auditoria para um servidor syslog externo, primeiro você deve configurar o servidor externo.

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 8192 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 20GB Registros locais de Registros de auditoria (localaudit.log) são mantidos em cada nó.



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 endpoints privados da API `audit-destinations`. Por exemplo, é possível usar diferentes servidores syslog para diferentes grupos de nós.

Acesse o assistente de configuração do servidor syslog

Passos

1. Selecione **CONFIGURATION Monitoring Audit and syslog Server**.

Audit and syslog server

Audit messages and logs record system activities and security events and are an essential tool for monitoring and troubleshooting.

Audit levels

Adjust audit levels to increase or decrease the type and number of audit messages recorded.

System	Normal
Storage	Error
Management	Normal
Client reads	Normal
Client writes	Normal

Audit protocol headers

Optionally, define any HTTP request headers you want to include in client read and write audit messages.

Header name 1

[Add another header](#)

Use external syslog server

By default, audit messages are saved on Admin Nodes and logs are saved on the nodes where they were generated. If you want to save audit messages and a subset of logs externally, configure an external syslog server.

i If you want to use an external syslog server, you must configure it first.

[Configure external syslog server](#)

If you want to change these log locations, select a different option below.

Log type	Log location
Audit log	Admin Nodes
Security events	Local nodes
Application logs	Local nodes

- Default (Admin Nodes/local nodes)
- External syslog server
- Admin Nodes and external syslog server
- Local nodes only

2. Na página servidor de auditoria e syslog, selecione **Configurar servidor syslog externo**. Se tiver configurado anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

Insira informações do syslog

Configure external syslog server

1 Enter syslog info

2 Manage syslog content

3 Send test messages

External syslog server configuration

Host ?

A valid FQDN or IP address.

Port ?

An integer between 1 and 65535.

Protocol ?

TCP TLS RELP/TCP RELP/TLS UDP

Server CA certificates ?

Client certificate ?

Client private key ?

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

TLS ou RELP/TLS é recomendado. 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, [Use os certificados de segurança do StorageGRID](#) consulte .

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



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

4. Selecione **continuar**.

5. se você selecionou **TLS** ou **RELP/TLS**, faça o upload dos 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. O arquivo que você carregar aqui pode ser um pacote de CA.
- **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.

- i. Selecione **Procurar** para o certificado ou chave que deseja usar.
- ii. Selecione o ficheiro de certificado ou o ficheiro de chave.
- iii. 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.

6. Selecione **continuar**.

Gerenciar o conteúdo do syslog

Configure external syslog server

✓ Enter syslog info

2 Manage syslog content

✓ Send test messages

Manage syslog content

Send audit logs ?

Severity ? Informational (6) ▼ Facility ? local7 (23) ▼

Send security events ?

Severity ? Passthrough ▼ Facility ? Passthrough ▼

Send application logs ?

Severity ? Passthrough ▼ Facility ? Passthrough ▼

Previous

Continue

1. Selecione cada tipo de informação de auditoria que pretende enviar para o servidor syslog externo.
 - * Enviar logs de auditoria*: Eventos do StorageGRID e atividades do sistema
 - **Enviar eventos de segurança**: Eventos de segurança, como quando um usuário não autorizado tenta entrar ou um usuário faz login como root
 - * Enviar logs de aplicativos*: Arquivos de log úteis para solução de problemas, incluindo:
 - bycast-err.log
 - bycast.log
 - jaeger.log
 - nms.log (somente nós administradores)
 - prometheus.log
 - raft.log
 - hagroups.log
2. Use os menus suspensos para selecionar a gravidade e a facilidade (tipo de mensagem) para a categoria de informações de auditoria que deseja enviar.

Se você selecionar **passagem** para gravidade e facilidade, as informações enviadas para o servidor syslog remoto receberão a mesma gravidade e facilidade que fez quando conectado localmente no nó. Definir facilidade e gravidade pode ajudá-lo a agregar os logs de maneiras personalizáveis para facilitar a análise.



Para obter mais informações sobre os logs do software StorageGRID, [Registos do software StorageGRID](#) consulte .

- a. Para **severidade**, selecione **passagem** se quiser que cada mensagem enviada para o syslog externo tenha o mesmo valor de gravidade que no syslog local.

Para logs de auditoria, se você selecionar **Passthrough**, a gravidade é 'info'.

Para eventos de segurança, se você selecionar **passagem**, os valores de gravidade serão gerados pela distribuição linux nos nós.

Para logs de aplicativos, se você selecionar **passagem**, 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'.

- b. Se não pretender utilizar o valor de passagem, selecione um valor de gravidade entre 0 e 7.

O valor selecionado será aplicado a todas as mensagens deste tipo. As informações sobre diferentes gravidades serão perdidas quando você optar por substituir a gravidade com um valor fixo.

Gravidade	Descrição
0	Emergência: O sistema não pode ser utilizado
1	Alerta: A ação deve ser tomada imediatamente
2	Crítico: Condições críticas
3	Erro: Condições de erro
4	Aviso: Condições de aviso
5	Aviso: Condição normal, mas significativa
6	Informativo: Mensagens informativas
7	Debug: Mensagens no nível de depuração

- c. Para **Facility**, selecione **Passthrough** se quiser que cada mensagem enviada para o syslog externo tenha o mesmo valor de instalação que faz no syslog local.

Para logs de auditoria, se você selecionar **passagem**, a facilidade enviada para o servidor syslog externo é 'local7'.

Para eventos de segurança, se você selecionar **passagem**, os valores das instalações serão gerados pela distribuição linux nos nós.

Para logs de aplicativos, se você selecionar **passagem**, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação:

Registo de aplicações	Valor de passagem
bycast.log	usuário ou daemon
bycast-err.log	usuário, daemon, local3 ou local4
jaeger.log	local2
nms.log	local3
prometheus.log	local4
raft.log	local5
hagroups.log	local6

d. Se você não quiser usar o valor de passagem, selecione o valor de instalação entre 0 e 23.

O valor selecionado será aplicado a todas as mensagens deste tipo. Informações sobre diferentes instalações serão perdidas quando você optar por substituir instalações com um valor fixo.

Instalação	Descrição
0	kern (mensagens do kernel)
1	utilizador (mensagens no nível do utilizador)
2	e-mail
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)
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

Instalação	Descrição
12	NTP
13	logaudit (auditoria de log)
14	alerta de registo (alerta de registo)
15	relógio (daemon de relógio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selecione **continuar**.

Enviar mensagens de teste

Configure external syslog server

✓ Enter syslog info

✓ Manage syslog content

3 Send test messages

Send test messages from all nodes

⚠ After updating the syslog server configuration, confirm that the external syslog server can receive test StorageGRID messages. If the test messages cannot be delivered and you use this configuration, you might lose important messages regarding StorageGRID events and activities.

Before using the syslog server configuration, confirm that all nodes can send messages to the external server. Select **Send test messages** and then check the syslog server. Make sure it receives a test message from each node in your grid. As required, correct any reported errors and try again.

Send test messages

Previous

Skip and finish

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.

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

É apresentado um banner verde indicando que a sua configuração foi guardada com sucesso.

2. Caso contrário, selecione **Enviar mensagens de teste**.

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, corrija-o e selecione **Enviar mensagens de teste** novamente. [Solução de problemas do 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 é exibido notificando que a configuração do servidor syslog foi salva com sucesso.



Suas 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 eventos de segurança, os logs de aplicativos e os logs de mensagens de auditoria são enviados.



Para obter mais informações sobre os logs do software StorageGRID, [Registros do software StorageGRID](#) consulte .

1. Na página servidor de auditoria e syslog, selecione o destino das informações de auditoria nas opções listadas:

Opção	Descrição
Padrão (nós de administração/nós locais)	As mensagens de auditoria são enviadas para o log de auditoria (<code>audit.log</code>) no Admin Node, e os logs de eventos de segurança e de aplicativos são armazenados nos nós em que foram gerados (também chamados de "o nó local").
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas no nó local. 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.
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (<code>audit.log</code>) no nó Admin e as informações de auditoria são enviadas para o servidor syslog externo e salvas no nó local. 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.
Somente nós locais	Nenhuma informação de auditoria é enviada para um Admin Node ou servidor syslog remoto. As informações de auditoria são salvas apenas nos nós que as geraram. Nota: O StorageGRID remove periodicamente esses 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.



As informações de auditoria geradas em cada nó local são armazenadas no `/var/local/log/localaudit.log`

1. Selecione **Guardar**. Em seguida, selecione OK para aceitar a alteração para o destino do log.
2. Se você selecionou **External syslog Server** ou **Admin Nodes e External syslog Server** como destino para informações de auditoria, um aviso adicional será exibido. Reveja o texto de aviso.



Você deve confirmar se o servidor syslog externo pode receber mensagens StorageGRID de teste.

1. Confirme se deseja alterar o destino para informações de auditoria selecionando **OK**.

Um banner verde é exibido notificando que sua configuração de auditoria foi salva com êxito.

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

Informações relacionadas

[Visão geral da mensagem de auditoria](#)

[Configurar mensagens de auditoria e destinos de log](#)

[Mensagens de auditoria do sistema](#)

[Mensagens de auditoria de armazenamento de objetos](#)

[Mensagem de auditoria de gerenciamento](#)

[O cliente lê mensagens de auditoria](#)

[Administrar o StorageGRID](#)

Utilize a monitorização SNMP

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 uma base de informações de gerenciamento (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.

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:

- **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** são semelhantes às armadilhas, 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 nos seguintes casos:

- 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. As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o 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 descrições dos alertas que podem acionar esses traps, consulte [Referência de alertas](#).

- Certos 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	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	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.

Acesse o MIB

Você pode acessar o arquivo de definição MIB no seguinte local em qualquer nó do StorageGRID:

```
/usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt
```

Informações relacionadas

- [Referência de alertas](#)
- [Referência de alarmes \(sistema legado\)](#)
- [Alarmes que geram notificações SNMP \(sistema legado\)](#)
- [Silenciar notificações de alerta](#)

Configure o agente SNMP

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

O que você vai precisar

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

Sobre esta tarefa

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Você pode configurar o agente para uma ou mais versões.

Passos

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

A página Agente SNMP é exibida.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP

Save

2. Para ativar o agente SNMP em todos os nós de grade, marque a caixa de seleção **Ativar SNMP**.

Os campos para configurar um agente SNMP são exibidos.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP

System Contact

System Location

Enable SNMP Agent Notifications

Enable Authentication Traps

Community Strings

Default Trap Community

Read-Only Community

String 1 +

Other Configurations

Agent Addresses (0) USM Users (0) Trap Destinations (0)

+ Create Edit x Remove

Internet Protocol	Transport Protocol	StorageGRID Network	Port
No results found.			

[Save](#)

3. No campo **Contato do sistema**, insira o valor que você deseja que o StorageGRID forneça nas mensagens SNMP para o sysContact.

Normalmente, o contacto do sistema é um endereço de correio eletrónico. O valor fornecido aplica-se a todos os nós do sistema StorageGRID. **O Contato do sistema** pode ter no máximo 255 caracteres.

4. No campo **localização do sistema**, insira o valor que você deseja que o StorageGRID forneça nas mensagens SNMP para sysLocation.

A localização do sistema pode ser qualquer informação útil para identificar onde o sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. O valor fornecido aplica-se a todos os nós do sistema StorageGRID. **A localização do sistema** pode ter no máximo 255 caracteres.

5. Mantenha a caixa de seleção **Ativar notificações de agentes SNMP** selecionada se desejar que o agente SNMP do StorageGRID envie uma armadilha e informe notificações.

Se esta caixa de verificação não estiver selecionada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

6. Marque a caixa de seleção **Enable Authentication traps** (Ativar traps de autenticação) se desejar que o agente SNMP do StorageGRID envie uma armadilha de autenticação se receber uma mensagem de

protocolo autenticada incorretamente.

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

Os campos nesta seção são usados para autenticação baseada na comunidade em SNMPv1 ou SNMPv2c. Esses campos não se aplicam ao SNMPv3.

- a. No campo **Default Trap Community** (Comunidade de Trap padrão), insira opcionalmente a cadeia de caracteres da comunidade padrão que você deseja usar para destinos de trap.

Conforme necessário, você pode fornecer uma string de comunidade diferente (" personalizado ") quando você [defina um destino específico da armadilha](#).

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

- b. Para **Comunidade somente leitura**, insira uma ou mais strings de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6. Clique no sinal de adição **+** para adicionar várias cadeias de caracteres.

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.

Cada string de comunidade pode ter no máximo 32 caracteres e não pode conter caracteres de espaço em branco. Até cinco cordas são permitidas.



Para garantir a segurança do seu sistema StorageGRID, não use "público" como a cadeia de caracteres da comunidade. Se você não inserir uma string de comunidade, o agente SNMP usará a ID de grade do seu sistema StorageGRID como a string de comunidade.

8. Opcionalmente, selecione a guia endereços de agentes na seção outras configurações .

Use esta guia para especificar um ou mais ""endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas. Cada endereço de agente inclui um protocolo de Internet, um protocolo de transporte, uma rede StorageGRID e, opcionalmente, uma porta.

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

- a. Clique em **criar**.

A caixa de diálogo criar endereço do agente é exibida.

Create Agent Address

Internet Protocol IPv4 IPv6

Transport Protocol UDP TCP

StorageGRID Network

Port

b. Para **Internet Protocol**, selecione se este endereço usará IPv4 ou IPv6.

Por padrão, o SNMP usa IPv4.

c. Para **Protocolo de Transporte**, selecione se este endereço usará UDP ou TCP.

Por padrão, o SNMP usa UDP.

d. No campo **rede StorageGRID**, selecione em qual rede StorageGRID a consulta será recebida.

- Rede, administrador e redes de clientes: O StorageGRID deve ouvir consultas SNMP em todas as três redes.
- Rede de rede
- Rede de administração
- Rede de clientes



Para garantir que as comunicações do cliente com o StorageGRID permaneçam seguras, você não deve criar um endereço de agente para a rede do cliente.

e. No campo **Port**, insira 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.



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.

f. Clique em **criar**.

O endereço do agente é criado e adicionado à tabela.

Other Configurations

Agent Addresses (2)

USM Users (2)

Trap Destinations (2)

<input type="button" value="+ Create"/>	<input type="button" value="✎ Edit"/>	<input type="button" value="✕ Remove"/>		
	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

9. Se estiver a utilizar o SNMPv3, selecione o separador utilizadores USM na secção outras configurações.

Utilize este separador para definir os utilizadores USM que estão autorizados a consultar a MIB ou a receber traps e informações.



Esta etapa não se aplica se você estiver usando apenas SNMPv1 ou SNMPv2c.

a. Clique em **criar**.

É apresentada a caixa de diálogo Create USM User (criar utilizador USM).

Create USM User

Username

Read-Only MIB Access

Authoritative Engine ID

Security Level authPriv authNoPriv

Authentication

Protocol

Password

Confirm Password

Privacy

Protocol

Password

Confirm Password

Cancel

Create

- b. Introduza um **Nome de utilizador** exclusivo para este utilizador USM.

Os nomes de usuário têm 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.

- c. Marque a caixa de seleção **Acesso MIB somente leitura** se esse usuário tiver acesso somente leitura à MIB.

Se você selecionar **Acesso MIB somente leitura**, o campo **ID do mecanismo autoritário** será desativado.



Os utilizadores USM que têm acesso MIB apenas de leitura não podem ter IDs de motor.

- d. Se este utilizador for utilizado num destino de informação, introduza o **ID de motor autoritário** para este utilizador.



SNMPv3 informar destinos devem ter usuários com IDs de motor. SNMPv3 o destino do trap não pode ter utilizadores com IDs de motor.

O ID oficial do mecanismo pode ser de 5 a 32 bytes em hexadecimal.

- e. Selecione um nível de segurança para o utilizador USM.

- **AuthPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe, um protocolo de privacidade e uma palavra-passe.
- **AuthNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe.

- f. Introduza e confirme a palavra-passe que este utilizador utilizará para autenticação.



O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).

- g. Se selecionou **authPriv**, introduza e confirme a palavra-passe que este utilizador utilizará para a privacidade.



O único protocolo de privacidade suportado é AES.

- h. Clique em **criar**.

O utilizador USM é criado e adicionado à tabela.

Other Configurations

Agent Addresses (2)

USM Users (3)

Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

10. na seção outras configurações, selecione a guia Trap Destinations.

A guia Destinos de armadilha permite definir um ou mais destinos para notificações de intercetação StorageGRID ou informar. Quando você ativa o agente SNMP e clica em **Salvar**, o StorageGRID começa a enviar notificações para cada destino definido. As notificações são enviadas quando alertas e alarmes são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

a. Clique em **criar**.

A caixa de diálogo criar destino de armadilha é exibida.

Create Trap Destination

Version SNMPv1 SNMPv2C SNMPv3

Type ⓘ Trap

Host ⓘ

Port ⓘ 162

Protocol ⓘ UDP TCP

Community String ⓘ Use the default trap community: No default found
(Specify the default on the SNMP Agent page.)
 Use a custom community string

Custom Community String

b. No campo **Version** (versão), selecione qual versão SNMP será utilizada para esta notificação.

c. Preencha o formulário, com base na versão selecionada

Versão	Especifique esta informação
SNMPv1	<p>Nota: para SNMPv1, o agente SNMP só pode enviar traps. As informações não são suportadas.</p> <ol style="list-style-type: none"> i. No campo Host, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. ii. Para Port, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iii. Para Protocolo, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) iv. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, ou insira uma string de comunidade personalizada para esse destino de trap. <p>A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaço em branco.</p>
SNMPv2c	<ol style="list-style-type: none"> i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo Host, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para Port, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para Protocolo, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, ou insira uma string de comunidade personalizada para esse destino de trap. <p>A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaço em branco.</p>

Versão	Especifique esta informação
SNMPv3	<ul style="list-style-type: none"> i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo Host, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para Port, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para Protocolo, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Selecione o utilizador USM que será utilizado para autenticação. <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.

d. Clique em **criar**.

O destino da armadilha é criado e adicionado à tabela.

Other Configurations

Agent Addresses (1) USM Users (2) **Trap Destinations (2)**

+ Create
✎ Edit
✖ Remove

	Version	Type	Host	Port	Protocol	Community/USM User
<input type="radio"/>	SNMPv3	Trap	local		UDP	User: Read only user
<input type="radio"/>	SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

11. Quando tiver concluído a configuração do agente SNMP, clique em **Save**

A nova configuração do agente SNMP fica ativa.

Informações relacionadas

[Silenciar notificações de alerta](#)

Atualize o agente SNMP

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

O que você vai precisar

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

Sobre esta tarefa

Sempre que atualizar o [Configuração do agente SNMP](#), tenha em atenção que tem de clicar em **Guardar** na parte inferior da página Agente SNMP para confirmar quaisquer alterações efetuadas em cada separador.

Passos

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

A página Agente SNMP é exibida.

2. Se quiser desativar o agente SNMP em todos os nós de grade, desmarque a caixa de seleção **Ativar SNMP** e clique em **Salvar**.

O agente SNMP está desativado para todos os nós de grade. Se você reativar o agente posteriormente, quaisquer configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize os valores inseridos para **Contato do sistema e localização do sistema**.
4. Opcionalmente, desmarque a caixa de seleção **Ativar notificações de agentes SNMP** se você não quiser mais que o agente SNMP do StorageGRID envie trap e informe notificações.

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

5. Opcionalmente, desmarque a caixa de seleção **Ativar traps de autenticação** se você não quiser mais que o agente SNMP do StorageGRID envie uma armadilha de autenticação quando receber uma mensagem de protocolo autenticada incorretamente.
6. Se você usar SNMPv1 ou SNMPv2c, atualize opcionalmente a seção cadeias de Comunidade.

Os campos nesta seção são usados para autenticação baseada na comunidade em SNMPv1 ou SNMPv2c. Esses campos não se aplicam ao SNMPv3.



Se você quiser remover a cadeia de caracteres padrão da comunidade, primeiro você deve garantir que todos os destinos de intercetação usem uma cadeia de caracteres personalizada da comunidade.

7. Se quiser atualizar endereços de agentes, selecione a guia endereços de agentes na seção outras configurações .

Other Configurations

Agent Addresses (2) USM Users (2) Trap Destinations (2)

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

Use esta guia para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas. Cada endereço de agente inclui um protocolo de Internet, um protocolo de transporte, uma rede StorageGRID e uma porta.

- Para adicionar um endereço de agente, clique em **criar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.
 - Para editar um endereço de agente, selecione o botão de opção para o endereço e clique em **Editar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.
 - Para remover um endereço de agente, selecione o botão de opção para o endereço e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover esse endereço.
 - Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.
8. Se pretender atualizar utilizadores USM, selecione o separador utilizadores USM na secção outras configurações.

Other Configurations

Agent Addresses (2) USM Users (3) Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	<input checked="" type="checkbox"/>	authNoPriv	
<input type="radio"/>	user1	<input type="checkbox"/>	authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3	<input type="checkbox"/>	authPriv	59D39E801256

Utilize este separador para definir os utilizadores USM que estão autorizados a consultar a MIB ou a receber traps e informações.

- Para adicionar um utilizador USM, clique em **criar**. Em seguida, consulte a etapa para usuários USM nas instruções para configurar o agente SNMP.
- Para editar um utilizador USM, selecione o botão de opção do utilizador e clique em **Edit**. Em seguida,

consulte a etapa para usuários USM nas instruções para configurar o agente SNMP.

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, edite ou remova o destino, conforme descrito na etapa [Destino de trap SNMP](#). Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

- c. Para remover um utilizador USM, selecione o botão de opção do utilizador e clique em **Remove**. Em seguida, clique em **OK** para confirmar que deseja remover esse usuário.



Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deverá editar ou remover o destino, conforme descrito na etapa [Destino de trap SNMP](#). Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Undefined trap destination usmUser 'user1'

OK

- a. Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.

9. se você quiser atualizar destinos de intercetação, selecione a guia Destinos de intercetação na seção outras configurações.

Other Configurations

Agent Addresses (1)

USM Users (2)

Trap Destinations (2)

+ Create Edit Remove						
Version	Type	Host	Port	Protocol	Community/USM User	
SNMPv3	Trap	local		UDP	User: Read only user	
SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user	

A guia Destinos de armadilha permite definir um ou mais destinos para notificações de intercetação StorageGRID ou informar. Quando você ativa o agente SNMP e clica em **Salvar**, o StorageGRID começa a enviar notificações para cada destino definido. As notificações são enviadas quando alertas e alarmes são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

- a. Para adicionar um destino de armadilha, clique em **criar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.
 - b. Para editar um destino de armadilha, selecione o botão de opção do usuário e clique em **Editar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.
 - c. Para remover um destino de armadilha, selecione o botão de opção para o destino e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover este destino.
 - d. Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.
10. Quando tiver atualizado a configuração do agente SNMP, clique em **Save**.

Colete dados adicionais do StorageGRID

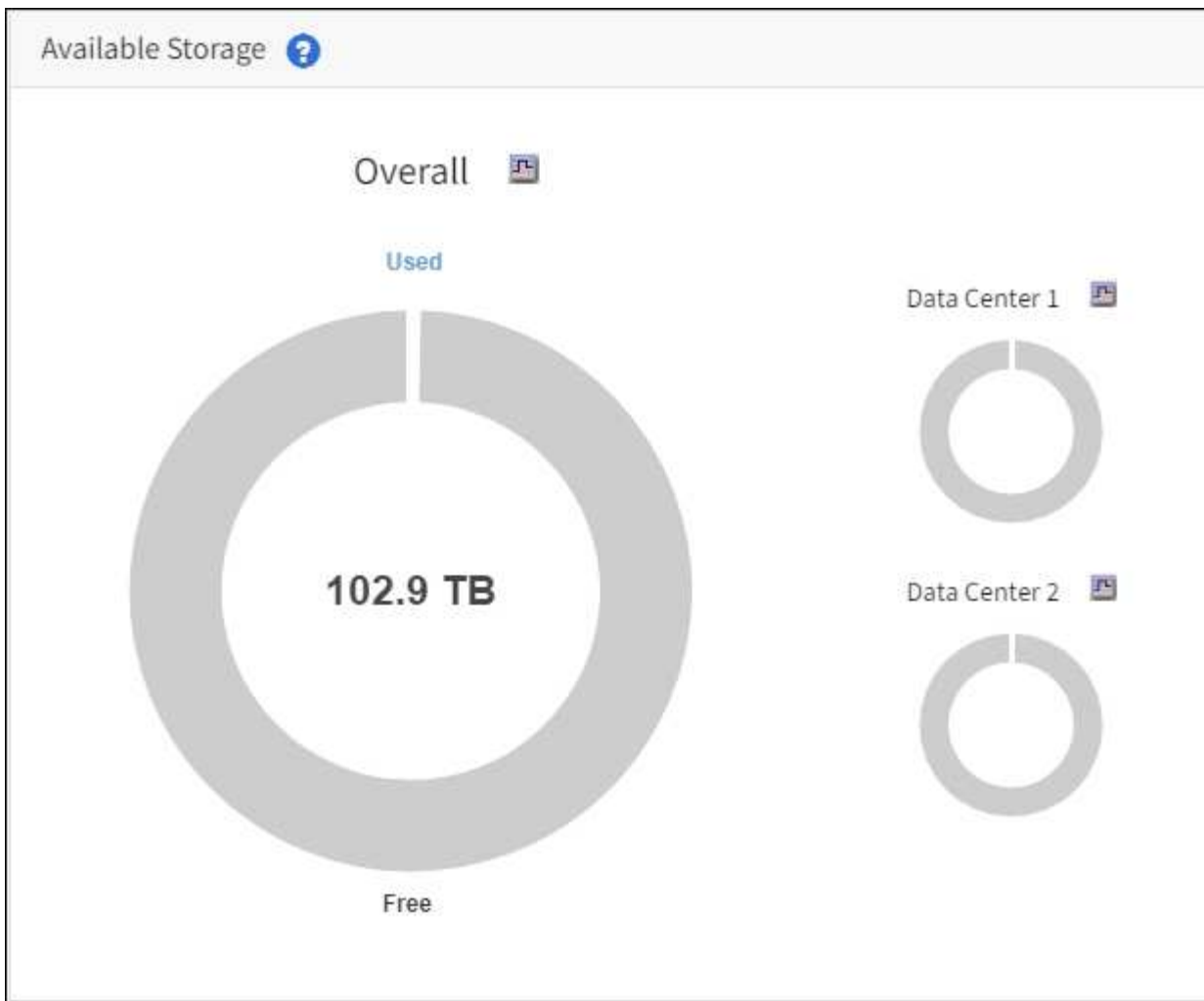
Use gráficos e gráficos

Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas. Os tipos de gráficos e relatórios disponíveis no Gerenciador de Grade incluem gráficos donut (somente no Painel), gráficos e relatórios de texto.

Tipos de gráficos

Gráficos e gráficos resumem os valores de métricas e atributos específicos do StorageGRID.

O Painel do Gerenciador de Grade inclui gráficos donut para resumir 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 **SUPORTE Ferramentas topologia de grade**.

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

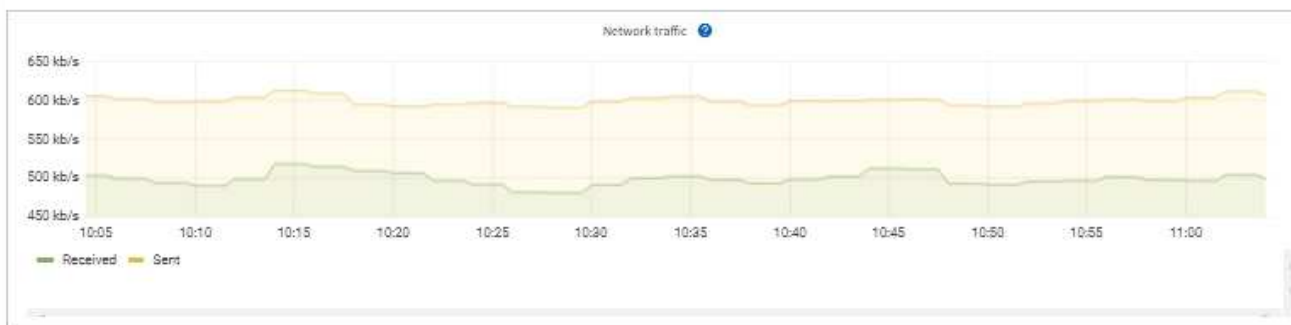
1 hour

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

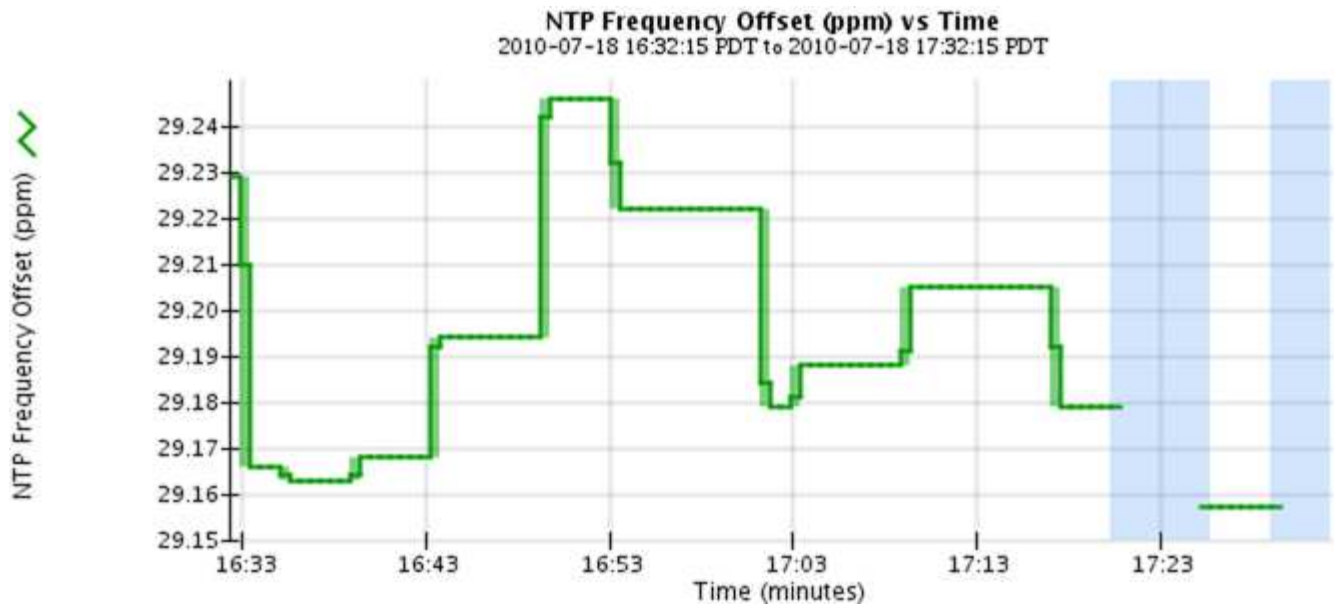
Transmit


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

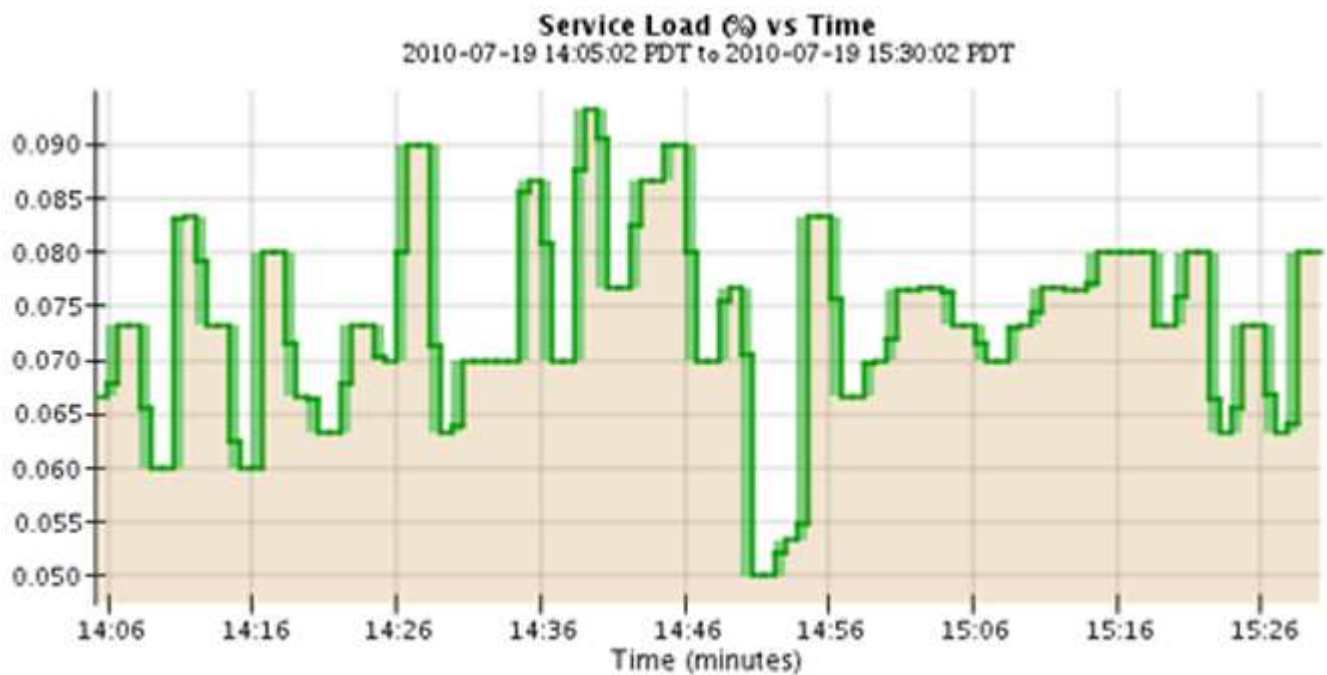


Gráficos Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPPORT Tools Metrics**.

- **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 traçar os valores dos atributos StorageGRID que têm um valor unitário (como o 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:


1 hour 1 day 1 week 1 month Custom

From: 2020-10-01 12 : 45 PM PDT

To: 2020-10-01 01 : 10 PM PDT Apply

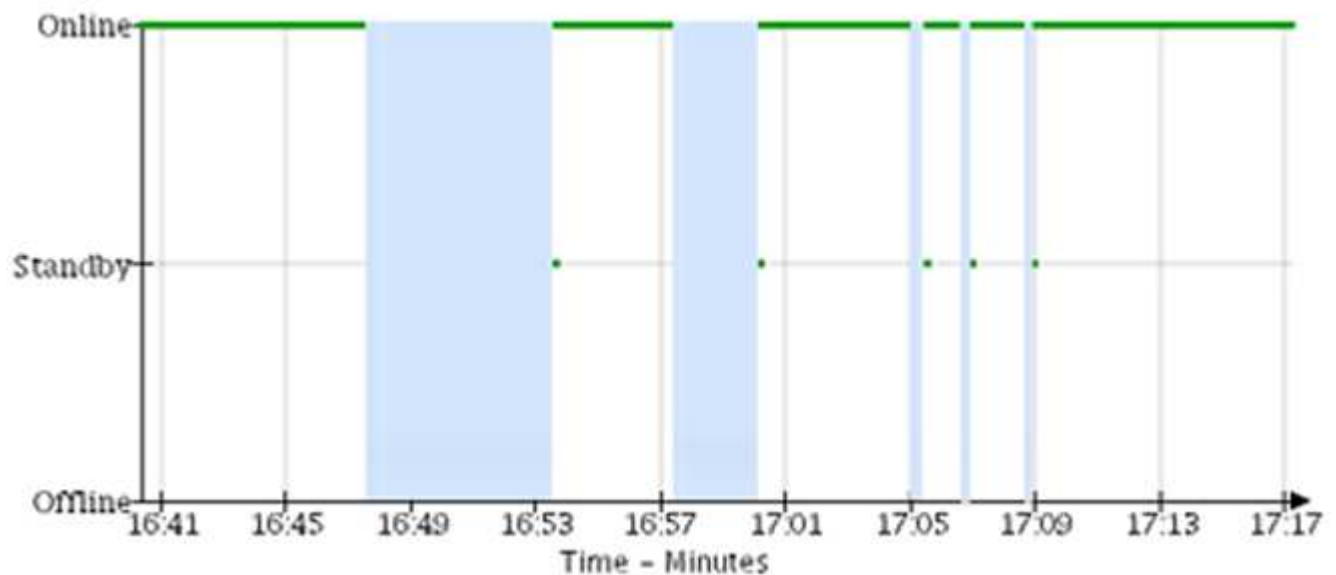


Close

- **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.

LDR State vs Time

2004-07-09 16:40:23 to 2004-07-09 17:17:11



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.

Amostra	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 "binned" 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.

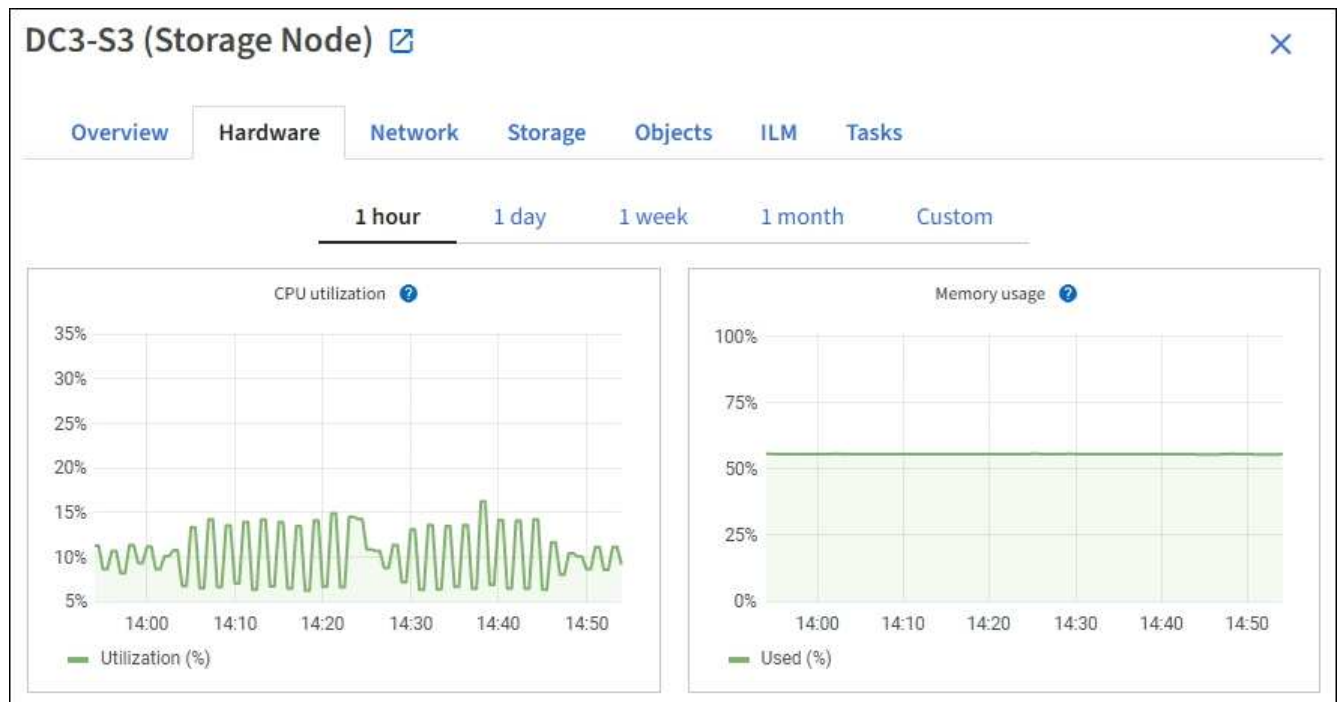
O que você vai precisar

Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

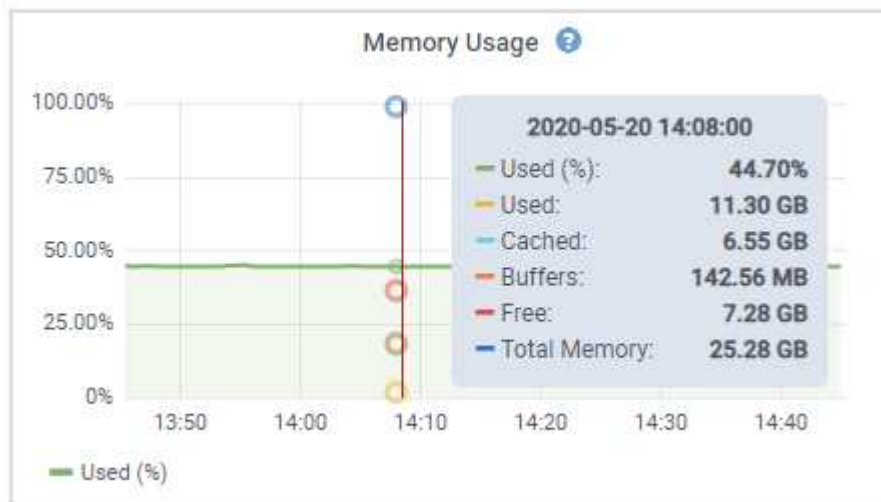
Passos


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** para um nó inclui dois gráficos Grafana.




3. Opcionalmente, passe 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.

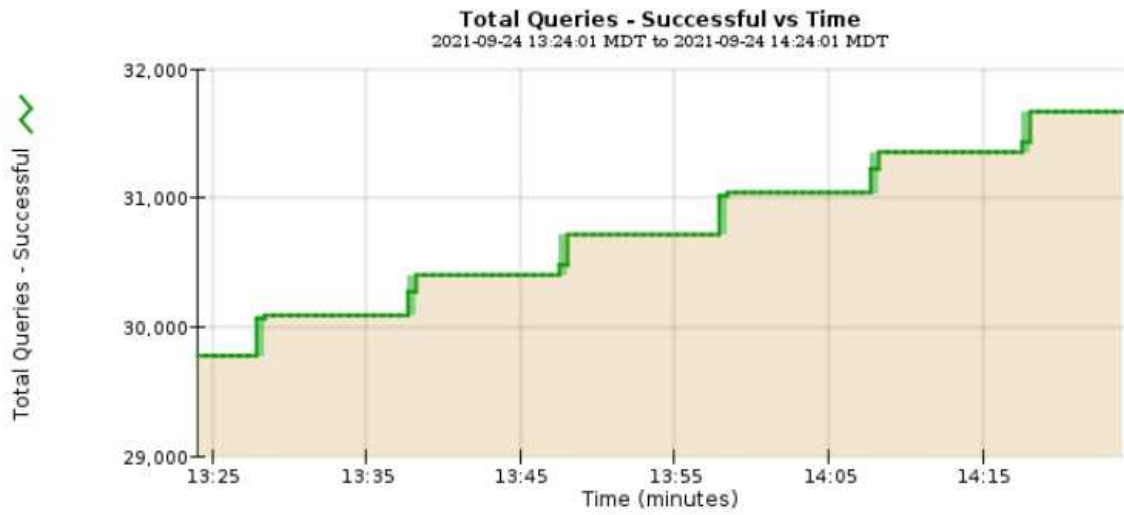


Os gráficos não estão disponíveis para todas as métricas e atributos.

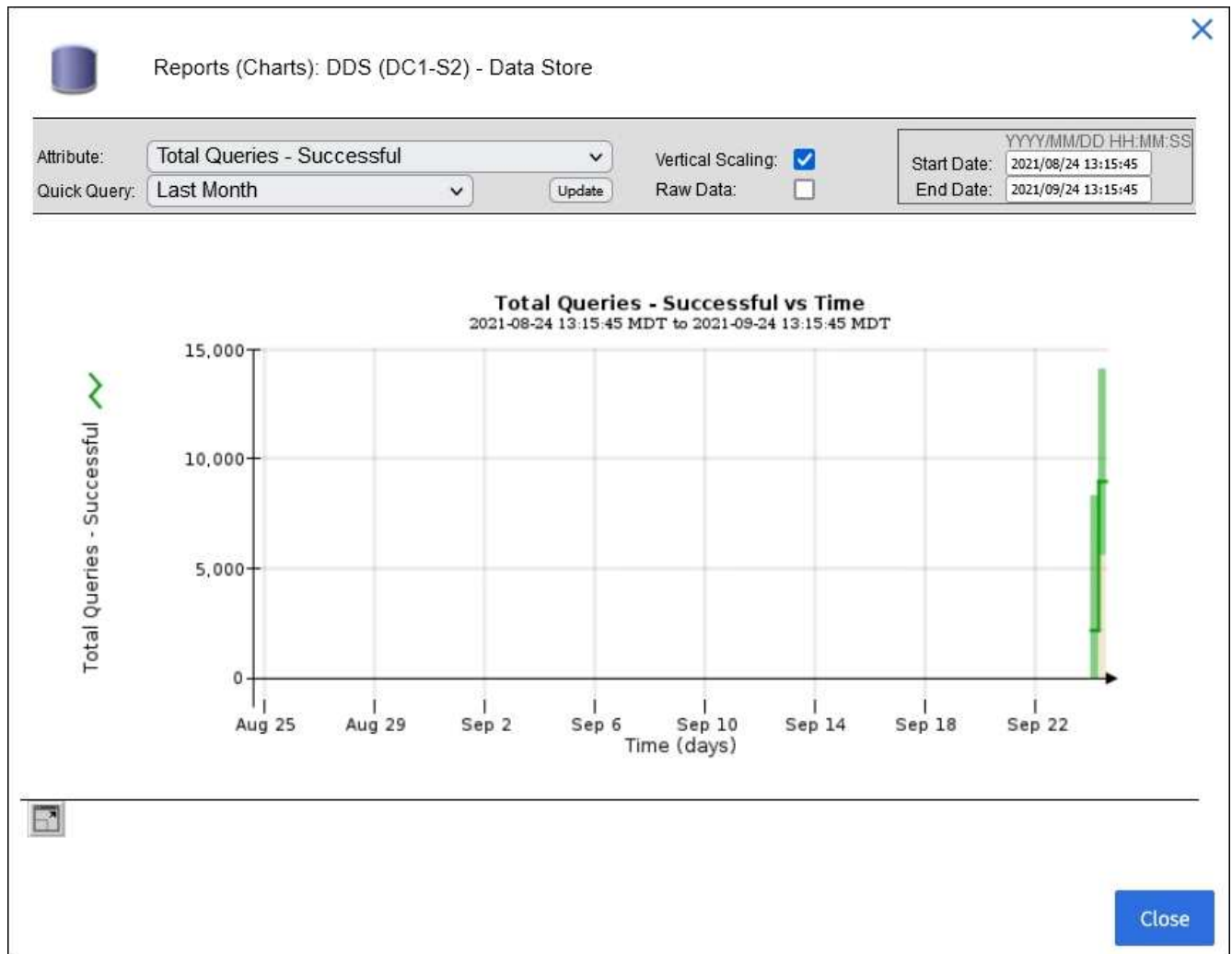
Exemplo 1: Na guia objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico  para ver o número total de consultas de armazenamento de metadados bem-sucedidas para o nó de armazenamento.




Attribute: Total Queries - Successful Vertical Scaling:
Quick Query: Last Hour Update Raw Data:
Start Date: 2021/09/24 13:24:01 End Date: 2021/09/24 14:24:01




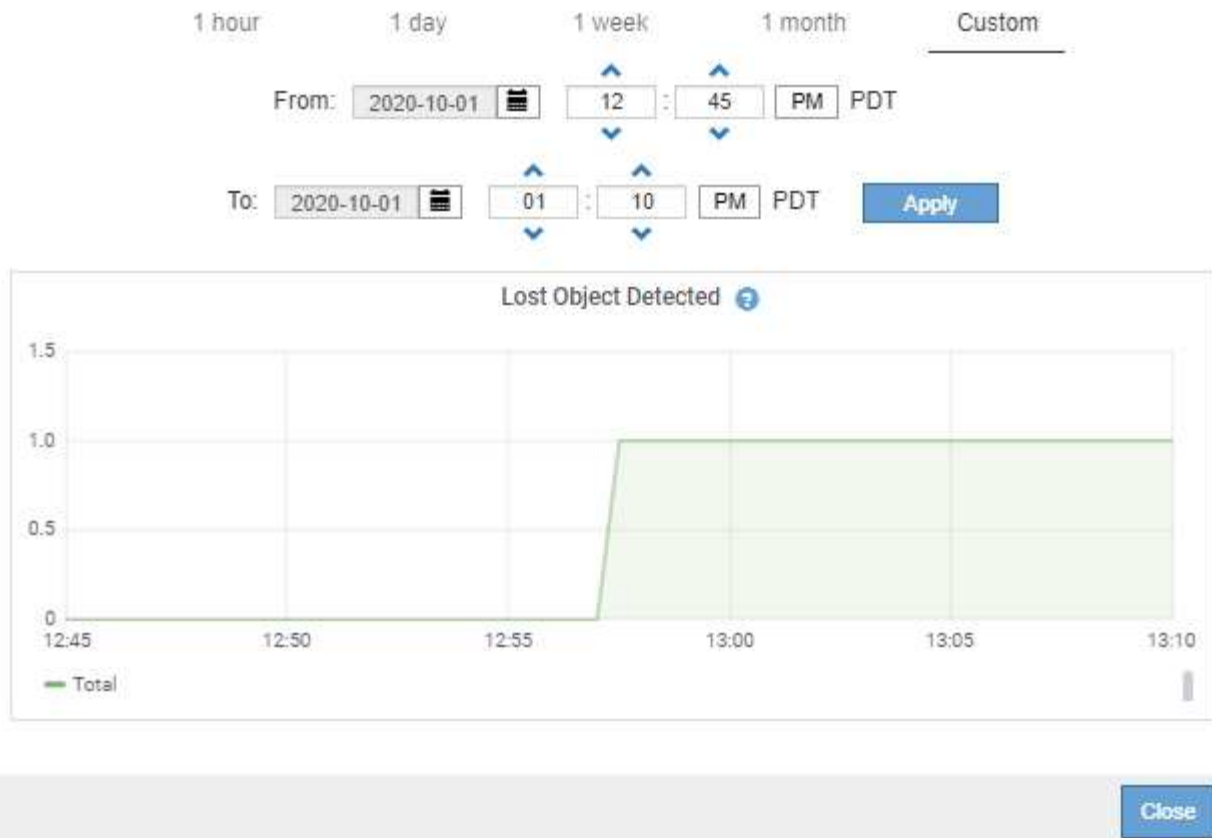
Close



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**.

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.

O que você vai precisar

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

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 relatados como porcentagens), desmarque a caixa de seleção **dados brutos**.

6. Selecione o período de tempo para relatar na lista suspensa **consulta rápida**.

Selecione a opção consulta personalizada para selecionar um intervalo de tempo específico.

O gráfico aparece 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 exhibe 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.

O que você vai precisar

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

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

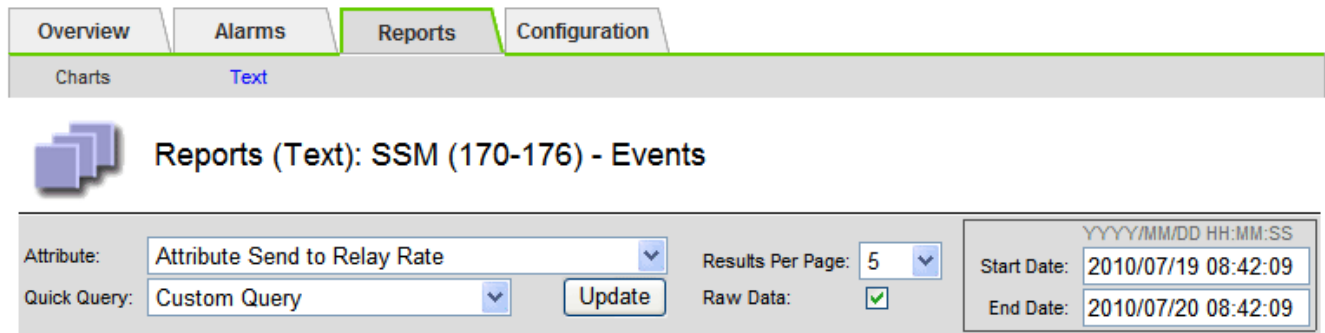
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

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*** .



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.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.

Sobre esta tarefa

Dois [processos de verificação](#) trabalham juntos para garantir a integridade dos dados:

- * A verificação em segundo plano* é executada automaticamente, verificando continuamente a correção dos dados do objeto.

A verificação em segundo plano verifica automaticamente e continuamente todos os nós de storage para determinar se há cópias corrompidas de dados de objetos replicados e codificados por apagamento. Se forem encontrados problemas, o sistema StorageGRID tentará substituir automaticamente os dados de objetos corrompidos de cópias armazenadas em outro lugar do sistema. A verificação em segundo plano não é executada em nós de arquivamento ou em objetos em um pool de storage de nuvem.



O alerta **Objeto corrompido não identificado detetado** é acionado se o sistema detetar um objeto corrompido que não pode ser corrigido automaticamente.

- **A verificação de existência de objetos** pode ser acionada por um usuário para verificar mais rapidamente a existência (embora não a correção) de dados de objetos.

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

Você deve rever os resultados de verificações de antecedentes e verificações de existência de objetos regularmente. Investigue quaisquer instâncias de dados de objetos corrompidos ou ausentes imediatamente para determinar a causa raiz.

Passos

1. Reveja os resultados das verificações de antecedentes:
 - a. Selecione **NÓS 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 em falta e o [Alerta de objetos perdidos](#) tiver sido acionado, contacte 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...

<input type="checkbox"/>	Job ID [?]	Status [⬇]	Nodes (volumes) [?]	Missing object copies detected [?]
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <u>7 more</u>	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**.

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

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

1. Selecione **SUPPORT Alarmes (legacy) Custom events**.

2. Clique em **Edit**  (ou **Insert**  se este não for o primeiro evento).
3. Introduza uma cadeia de eventos personalizada, por exemplo, encerramento




The screenshot shows a web interface for managing events. At the top left, there is a small icon and the title "Events" with a timestamp "Updated: 2021-10-22 11:15:34 MDT". Below this, the text "Custom Events (1 - 1 of 1)" is displayed. A table with two columns, "Event" and "Actions", is shown. The "Event" column contains the text "shutdown". The "Actions" column contains four icons: a pencil, a plus sign, a minus sign, and a hand. Below the table, there is a "Show 10 Records Per Page" dropdown menu, a "Refresh" button, and navigation links for "Previous" and "Next" with a page number "1". At the bottom right, there is an "Apply Changes" button with a right-pointing arrow icon.

4. Selecione **aplicar alterações**.
5. Selecione **SUPPORT > Tools > Grid topology**.
6. Selecione **grid node SSM Events**.
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.

Sobre esta tarefa

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.

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 o acesso do cliente ao compartilhamento de auditoria para NFS e CIFS (CIFS está obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

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 .

Para obter detalhes sobre o arquivo de log de auditoria, o formato das mensagens de auditoria, os tipos de mensagens de auditoria e as ferramentas disponíveis para analisar mensagens de auditoria, consulte as instruções para mensagens de auditoria. Para saber como configurar o acesso de cliente de auditoria, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

[Rever registros de auditoria](#)

[Administrar o StorageGRID](#)

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.

O que você vai precisar

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

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente uma mensagem AutoSupport a ser enviada.

O que você vai precisar

- 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**.

A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Selecione **Enviar AutoSupport acionado pelo usuário**.

O StorageGRID tenta enviar uma mensagem do AutoSupport para o suporte técnico. 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 a mensagem AutoSupport novamente.



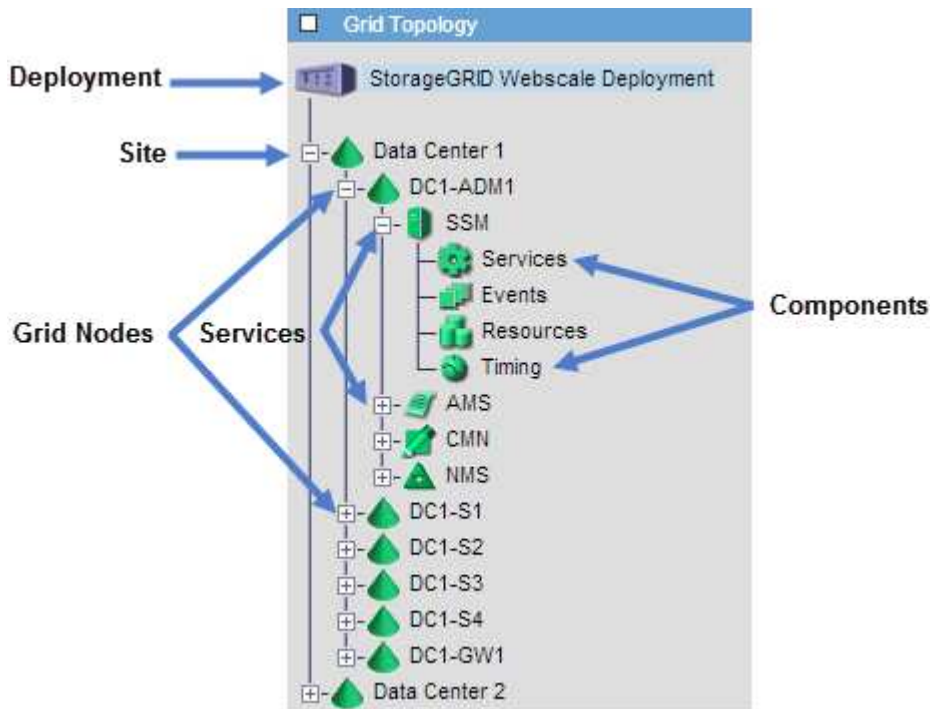
Depois de enviar uma mensagem AutoSupport acionada pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Informações relacionadas

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.

Analise as métricas de suporte

Ao solucionar um problema, você pode trabalhar com suporte técnico para analisar métricas e gráficos detalhados do seu sistema StorageGRID.

O que você vai precisar

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

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 **SUPORTE Ferramentas métricas**.

Um exemplo da página Metrics é mostrado aqui:

The screenshot shows the 'Metrics' page with the following content:

Metrics

Access charts and metrics to help troubleshoot issues.

i 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://storagegrid.com/metrics/graph>

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	Grid	S3 - Node
Account Service Overview	ILM	S3 Overview
Alertmanager	Identity Service Overview	S3 Select
Audit Overview	Ingests	Site
Cassandra Cluster Overview	Node	Support
Cassandra Network Overview	Node (Internal Use)	Traces
Cassandra Node Overview	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	
EC Overview	Replicated Read Path Overview	

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.

Enable query history

Expression (press Shift+Enter for newlines)

Execute

- insert metric at cursor -

Graph

Console

Element

Value

no data

[Remove Graph](#)

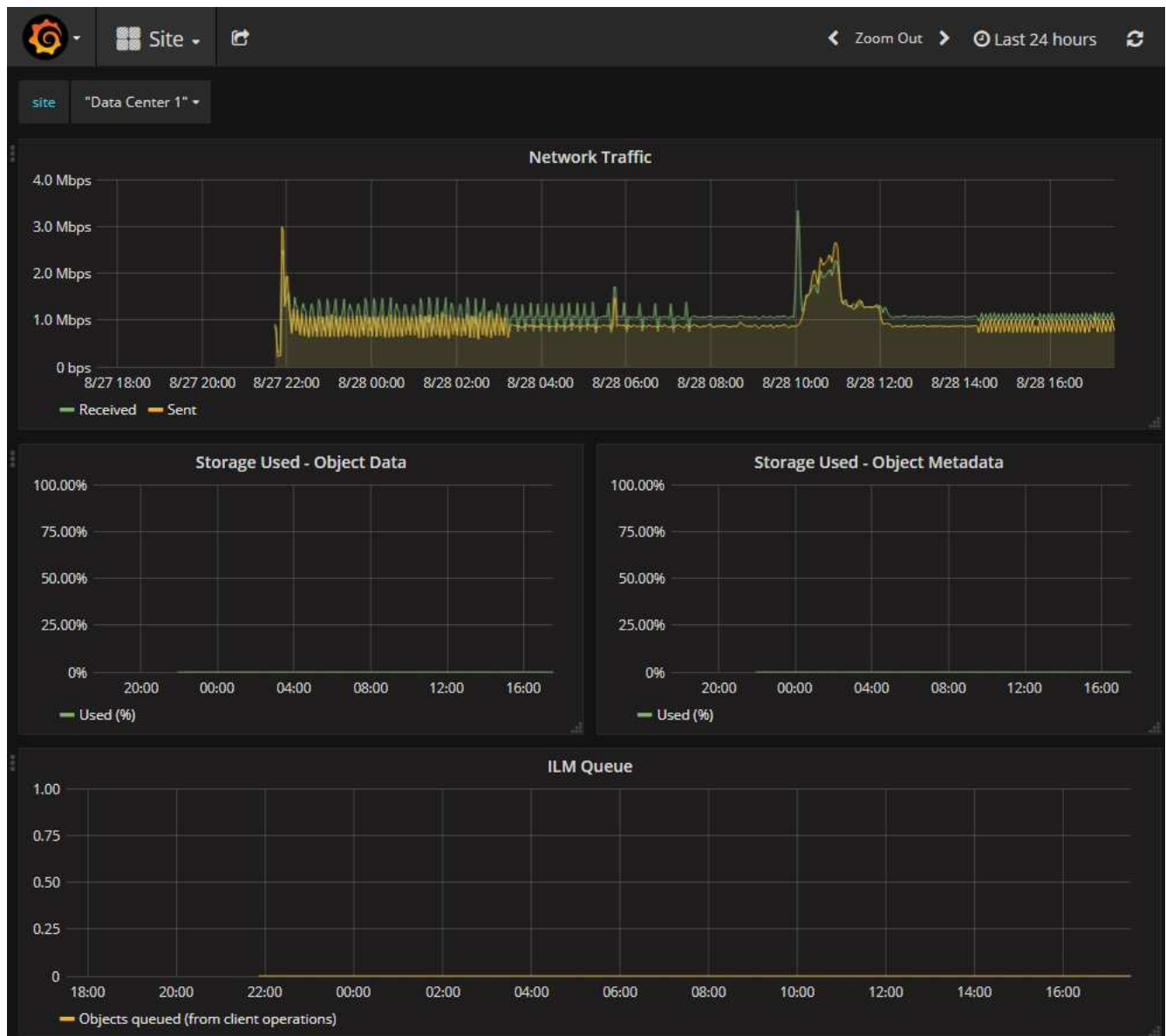
Add Graph



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](#)

O que você vai precisar

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

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 blocked task queue too large** ▾
- ✓ **Cassandra commit log latency** ▾
- ✓ **Cassandra commit log queue depth** ▾
- ✓ **Cassandra compaction queue too large** ▾

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.)
- **Limites:** Se disponíveis para o diagnóstico, os limites definidos pelo sistema para cada estado de diagnóstico anormal. (Os valores 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.

✓ **CPU utilization** ^

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`
[View in Prometheus](#) ↗

Thresholds

- ⚠ Attention >= 75%
- ✖ Caution >= 95%

Status	Instance	CPU Utilization
✓	DC1-ADM1	2.598%
✓	DC1-ARC1	0.937%
✓	DC1-G1	2.119%
✓	DC1-S1	8.708%
✓	DC1-S2	8.142%
✓	DC1-S3	9.669%
✓	DC2-ADM1	2.515%
✓	DC2-ARC1	1.152%
✓	DC2-S1	8.204%
✓	DC2-S2	5.000%
✓	DC2-S3	10.469%

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 **SUPORTE Ferramentas métricas**.



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))
```

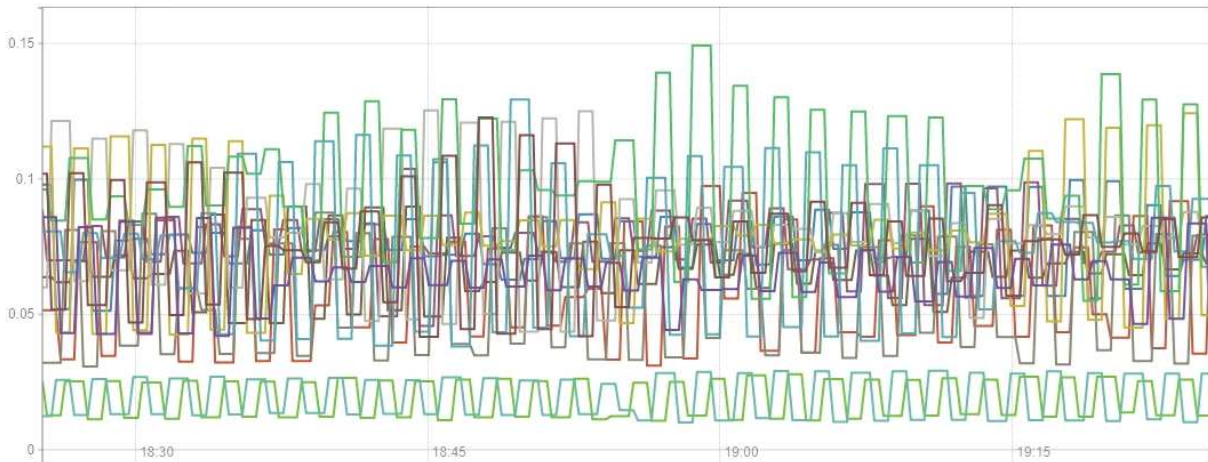
Load time: 547ms
Resolution: 14s
Total time series: 13

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.

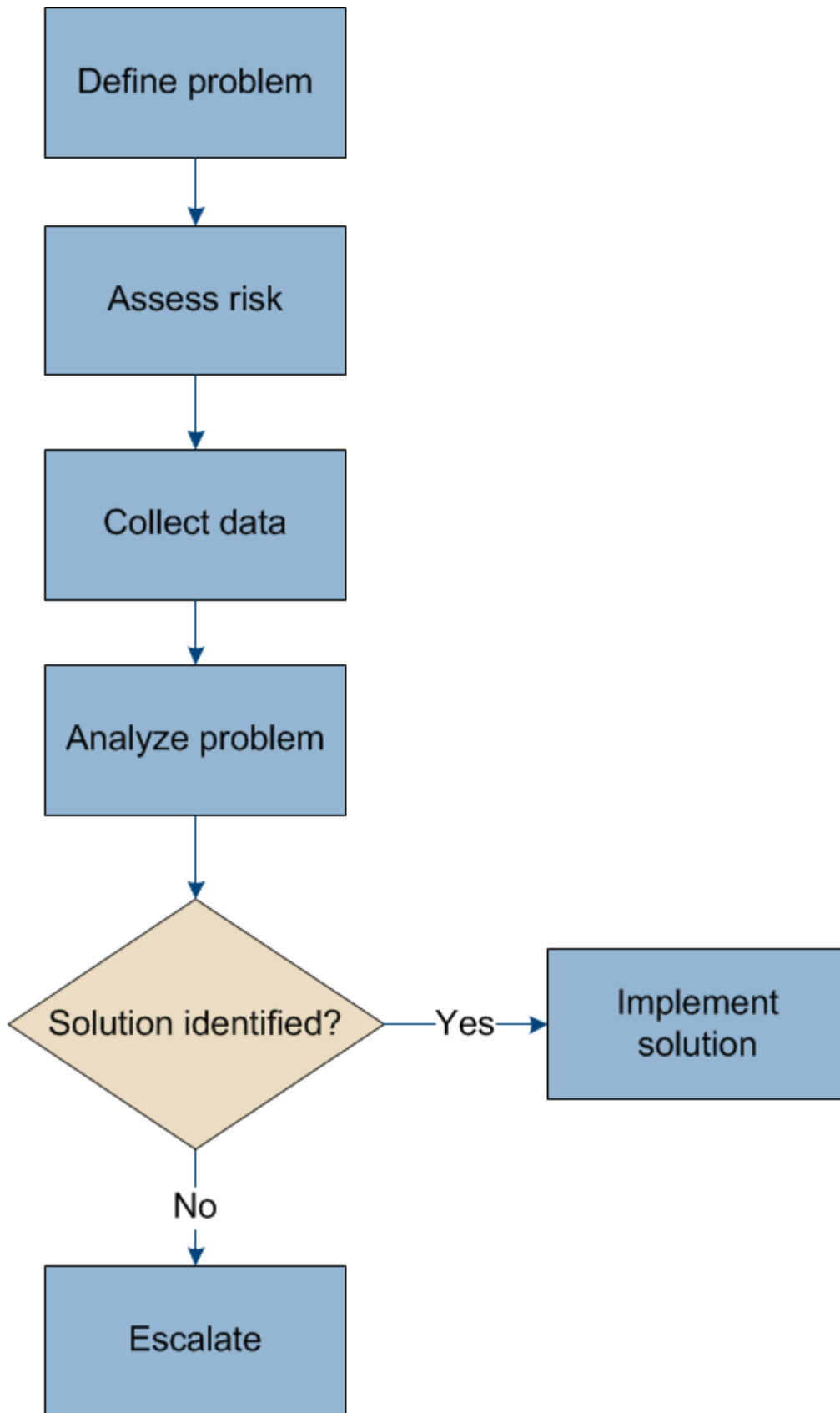
Solucionar problemas de um sistema StorageGRID

Solucionar problemas de um sistema StorageGRID

Se você encontrar um problema ao usar um sistema StorageGRID, consulte as dicas e diretrizes nesta seção para obter ajuda para determinar e resolver o problema.

Visão geral da determinação do problema

Se encontrar um problema quando [Administrar um sistema StorageGRID](#), pode utilizar o processo descrito nesta figura para identificar e analisar o problema. Em muitos casos, você pode resolver problemas sozinho. No entanto, talvez seja necessário encaminhar alguns problemas para o suporte técnico.



Defina o problema

O primeiro passo para resolver um problema é definir o problema claramente.

Esta tabela fornece exemplos dos tipos de informações que você pode coletar para definir um problema:

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

Avaliar o risco e o impactos no sistema

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

Esta tabela resume o impactos que o problema de exemplo está tendo nas operações do sistema:

Pergunta	Resposta da amostra
O sistema StorageGRID pode ingerir conteúdo?	Não
Os aplicativos clientes podem recuperar conteúdo?	Alguns objetos podem ser recuperados e outros não podem.
Os dados estão em risco?	Não
A capacidade de conduzir negócios é severamente afetada?	Sim, porque os aplicativos cliente não podem armazenar objetos no sistema StorageGRID e os dados não podem ser recuperados de forma consistente.

Coletar dados

Depois de definir o problema e avaliar o seu risco e impactos, recolha dados para análise. O tipo de dados que é mais útil para coletar depende da natureza do problema.

Tipo de dados a recolher	Por que coletar este dat	Instruções
Crie a linha do tempo das mudanças recentes	As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.	<ul style="list-style-type: none">• Crie uma linha do tempo das mudanças recentes
Reveja alertas e alarmes	<p>Alertas e alarmes podem ajudá-lo a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso.</p> <p>Revise a lista de alertas e alarmes atuais para ver se o StorageGRID identificou a causa raiz de um problema para você.</p> <p>Reveja alertas e alarmes acionados no passado para obter informações adicionais.</p>	<ul style="list-style-type: none">• Ver alertas atuais• Ver alarmes legados• Exibir alertas resolvidos• Rever alarmes históricos e frequência de alarmes (sistema legado)
Monitorar eventos	Os eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	<ul style="list-style-type: none">• Monitorar eventos
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas apareceram pela primeira vez e podem ajudá-lo a entender a rapidez com que as coisas estão mudando.	<ul style="list-style-type: none">• Use gráficos e gráficos• Use relatórios de texto
Estabeleça linhas de base	Recolher informações sobre os níveis normais de vários valores operacionais. Esses valores de linha de base, e desvios dessas linhas de base, podem fornecer pistas valiosas.	<ul style="list-style-type: none">• Estabeleça linhas de base
Execute testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com os vistos ao usar o aplicativo cliente.	<ul style="list-style-type: none">• Monitore O PUT e obtenha desempenho
Rever mensagens de auditoria	Revise as mensagens de auditoria para seguir as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	<ul style="list-style-type: none">• Rever mensagens de auditoria

Tipo de dados a recolher	Por que coletar este dat	Instruções
Verifique os locais dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de storage.	<ul style="list-style-type: none"> • Monitorar operações de verificação de objetos • Confirmar localizações de dados do objeto • Verifique a integridade do objeto
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	<ul style="list-style-type: none"> • Colete arquivos de log e dados do sistema • Acione manualmente uma mensagem AutoSupport • Analise as métricas de suporte

Crie uma linha do tempo de mudanças recentes

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

- As alterações ao seu sistema StorageGRID, à sua configuração ou ao seu ambiente podem causar um novo comportamento.
- Uma linha do tempo de mudanças pode ajudá-lo a identificar quais mudanças podem ser responsáveis por um problema e como cada mudança pode ter afetado seu desenvolvimento.

Crie uma tabela de alterações recentes no seu sistema que inclua informações sobre quando cada alteração ocorreu e quaisquer detalhes relevantes sobre a alteração, tais informações sobre o que mais estava acontecendo enquanto a mudança estava em andamento:

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

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi recentemente instalado, expandido ou recuperado?
- O sistema foi atualizado recentemente? Foi aplicado um hotfix?
- Algum hardware foi reparado ou alterado recentemente?
- A política ILM foi atualizada?
- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento mudou?
- Você alterou balanceadores de carga ou adicionou ou removeu um grupo de alta disponibilidade de nós de administrador ou nós de gateway?
- Foram iniciadas tarefas que podem demorar muito tempo a concluir? Os exemplos incluem:
 - Recuperação de um nó de storage com falha
 - Desativação do nó de storage
- Alguma alteração foi feita à autenticação do usuário, como adicionar um locatário ou alterar a configuração LDAP?
- A migração de dados está ocorrendo?
- Os serviços de plataforma foram recentemente ativados ou alterados?
- A conformidade foi ativada recentemente?
- Os pools de armazenamento em nuvem foram adicionados ou removidos?
- Alguma alteração foi feita na compactação ou criptografia de armazenamento?
- Houve alguma alteração na infra-estrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Alguma alteração foi feita em fontes NTP?
- Alguma alteração foi feita nas interfaces Grid, Admin ou Client Network?

- Alguma alteração de configuração foi feita no nó Arquivo?
- Alguma outra alteração foi feita ao sistema StorageGRID ou ao seu ambiente?

estabeleça linhas de base

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

Propriedade	Valor	Como obter
Consumo médio de storage	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - dados do objeto, encontre um período em que a linha esteja razoavelmente estável. Passe o cursor sobre o gráfico para estimar a quantidade de armazenamento consumida todos os dias Você pode coletar essas informações para todo o sistema ou para um data center específico.
Consumo médio de metadados	GB consumido/dia Percentagem consumida/dia	Vá para o Gerenciador de Grade. Na página nós, selecione toda a grade ou um site e vá para a guia armazenamento. No gráfico armazenamento usado - metadados de objetos, encontre um período em que a linha esteja razoavelmente estável. Passe o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido diariamente Você pode coletar essas informações para todo o sistema ou para um data center específico.

Propriedade	Valor	Como obter
Taxa de operações S3/Swift	Operações/segundo	<p>Vá para o Painel no Gerenciador de Grade. Na seção Protocol Operations (operações de protocolo), visualize os valores da taxa S3 e da taxa Swift.</p> <p>Para ver as taxas de ingestão e recuperação e contagens para um site ou nó específico, selecione NÓS site ou nó de armazenamento objetos. Passe o cursor sobre o gráfico de ingestão e recuperação para S3 ou Swift.</p>
Falha nas operações S3/Swift	Operações	<p>Selecione SUPPORT Tools Grid topology. Na guia Visão geral na seção operações da API, veja o valor de operações S3 - Falha ou operações rápidas - Falha.</p>
Taxa de avaliação ILM	Objetos/segundo	<p>Na página nós, selecione grid ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Passe o cursor sobre o gráfico para estimar um valor de linha de base para taxa de avaliação para o seu sistema.</p>
Taxa de digitalização ILM	Objetos/segundo	<p>Selecione NODES grid ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Passe o cursor sobre o gráfico para estimar um valor de linha de base para taxa de digitalização para o seu sistema.</p>
Objetos enfileirados de operações do cliente	Objetos/segundo	<p>Selecione NODES grid ILM.</p> <p>No gráfico fila ILM, encontre um período em que a linha esteja razoavelmente estável. Passe o cursor sobre o gráfico para estimar um valor de linha de base para objetos enfileirados (de operações do cliente) para o seu sistema.</p>

Propriedade	Valor	Como obter
Latência média da consulta	Milissegundos	Selecione NÓS Storage Node Objects . Na tabela consultas, exiba o valor da latência média.

Analisar dados


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

A análise é dependente de problemas, mas em geral:

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

Lista de verificação de informações de encaminhamento

Se você não conseguir resolver o problema sozinho, entre em Contato com o suporte técnico. Antes de entrar em Contato com o suporte técnico, reúna as informações listadas na tabela a seguir para facilitar a resolução de problemas.

	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, que horas ocorreu? Defina o problema
	Avaliação de impactos	Qual é a gravidade do problema? Qual é o impactos na aplicação cliente? <ul style="list-style-type: none"> • O cliente foi conetado com sucesso antes? • O cliente pode obter, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione MANUTENÇÃO sistema Licença . A ID do sistema StorageGRID é apresentada como parte da licença atual.
	Versão do software	Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione sobre para ver a versão do StorageGRID.

✓	Item	Notas
	Personalização	<p>Resumir como o seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte:</p> <ul style="list-style-type: none"> • A grade usa compactação de storage, criptografia de storage ou conformidade? • O ILM faz objetos replicados ou codificados para apagamento? O ILM garante a redundância do site? As regras do ILM usam os comportamentos de ingestão estritos, balanceados ou Dual Commit?
	Ficheiros de registo e dados do sistema	<p>Recolha ficheiros de registo e dados do sistema para o seu sistema. Selecione SUPPORT Tools Logs.</p> <p>Você pode coletar logs para toda a grade ou para nós selecionados.</p> <p>Se você estiver coletando logs somente para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de storage em um local incluem o serviço ADC.)</p> <p>Colete arquivos de log e dados do sistema</p>
	Informações da linha de base	<p>Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento.</p> <p>Estabeleça linhas de base</p>
	Cronograma das mudanças recentes	<p>Crie uma linha do tempo que resume quaisquer alterações recentes ao sistema ou ao seu ambiente.</p> <p>Crie uma linha do tempo das mudanças recentes</p>
	Histórico de esforços para diagnosticar o problema	<p>Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, certifique-se de Registrar as etapas que você tomou e o resultado.</p>

Solucionar problemas de objetos e storage

Confirmar localizações de dados do objeto

Dependendo do problema, você pode querer confirmar onde os dados do objeto estão sendo armazenados. Por exemplo, você pode querer verificar se a política ILM está funcionando como esperado e os dados do objeto estão sendo armazenados onde se pretende.

O que você vai precisar

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

Passos

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

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

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

Object Metadata Lookup

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

Identifier	<input type="text" value="source/testobject"/>
Version ID (optional)	<input type="text" value="MEJGMkMyQzgtNEY5OC0xMUU3LTkzMEYtRDkyNTAwQkY5I"/>

4. Selecione **Procurar**.

Os resultados da pesquisa de metadados de objeto aparecem. Esta página lista os seguintes tipos de informações:

- Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), o nome do objeto, o nome do contentor, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
- Para cópias de objetos replicadas, o local de storage atual de cada cópia.
- Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket

externo e o identificador exclusivo do objeto.

- Para objetos segmentados e objetos de várias partes, uma lista de segmentos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os primeiros 100 segmentos são mostrados.
- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não são garantidos para persistir de liberação para liberação.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Informações relacionadas

[Gerenciar objetos com ILM](#)

[Use S3](#)










[Use Swift](#)

Falhas no armazenamento de objetos (volume de storage)




















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

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






























Disk devices

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

Volumes

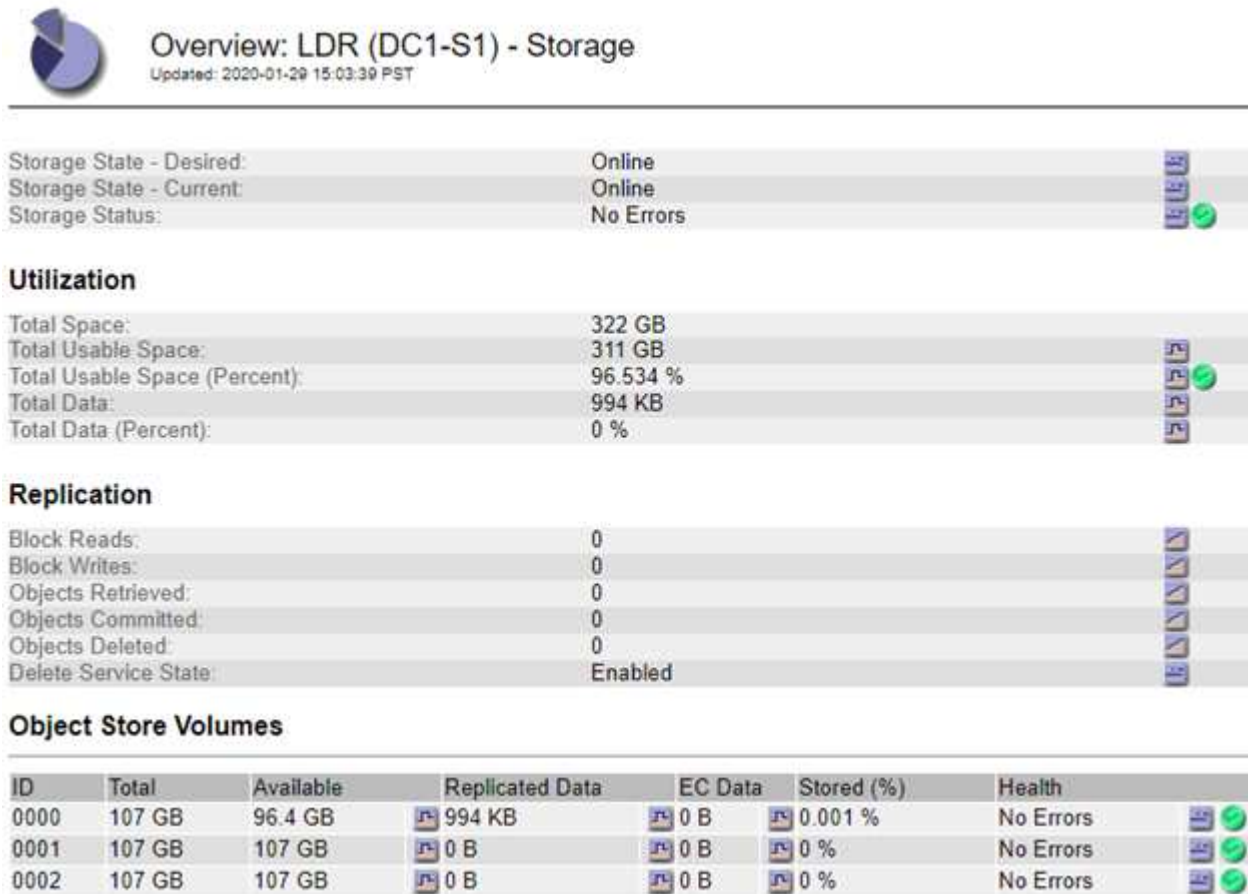
Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2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

Object stores

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

Para ver mais detalhes sobre cada nó de storage, siga estas etapas:

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



Overview: LDR (DC1-S1) - Storage
Updated: 2020-01-29 15:03:39 PST

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

Utilization

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

Replication

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

Object Store Volumes

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

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

Informações relacionadas

[Recuperar e manter](#)

Verifique a integridade do objeto

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

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

O que é a verificação em segundo plano?

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

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

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



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

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

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

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

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

Se o sistema detectar um objeto corrompido que não possa corrigir automaticamente (porque a corrupção impede que o objeto seja identificado), o alerta **Objeto corrompido não identificado detectado** é acionado.

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

Altere a taxa de verificação em segundo plano

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

O que você vai precisar

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

Sobre esta tarefa

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

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

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

Passos

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

Overview Alarms Reports Configuration

Main

Configuration: LDR (Storage Node Object) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count

Background Verification

Verification Rate Adaptive

Reset Corrupt Objects Count

Quarantined Objects

Delete Quarantined Objects

Apply Changes



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

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

Se a verificação em segundo plano encontrar dados de objeto replicados corrompidos, a métrica

objetos corrompidos será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte forma:

- Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar do sistema StorageGRID que satisfaça a política ILM ativa.
- Se o identificador de objeto não puder ser extraído (porque foi corrompido), a métrica **objetos corrompidos não identificados** é incrementada e o alerta **Objeto corrompido não identificado detetado** é acionado.

c. Se forem encontrados dados de objeto replicados corrompidos, entre em Contato com o suporte técnico para determinar a causa raiz da corrupção.

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

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

a. Selecione **SUPPORT > Tools > Grid topology**.

b. Selecione **Storage Node LDR Erasure Coding**.

c. Na tabela resultados da verificação, monitore o atributo fragmentos corrompidos detetados (ECCD).

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

a. Selecione **SUPPORT > Tools > Grid topology**.

b. Selecione **Storage Node LDR Verificação Configuração**.

c. Selecione **Redefinir contagem de objetos corrompidos**.

d. Clique em **aplicar alterações**.

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



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

a. Selecione **SUPPORT > Tools > Grid topology**.

b. Selecione **Storage Node LDR Verificação Configuração**.

c. Selecione **Excluir objetos em quarentena**.

d. Selecione **aplicar alterações**.

O que é verificação de existência de objeto?

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

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

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

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

Executar verificação de existência de objeto

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

O que você vai precisar

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

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

Sobre esta tarefa

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

Passos

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

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

Você pode pesquisar por nome do nó ou site.

Não é possível selecionar nós que não estão conectados à grade.

4. Selecione **continuar**.

5. Selecione um ou mais volumes para cada nó na lista. Você pode pesquisar volumes usando o número do volume de armazenamento ou o nome do nó.

Para selecionar todos os volumes para cada nó selecionado, marque a caixa de seleção **volume de armazenamento** no cabeçalho da coluna.

6. Selecione **continuar**.

7. Selecione o controle de consistência do trabalho.

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

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

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

8. Selecione **continuar**.

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

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

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



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

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

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

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

Object existence check

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

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

Active job Job history

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

Pause Cancel

Volumes Details

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

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

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

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

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

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

perdidas.

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

Object existence check

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

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

Active job | Job history

Delete | Rerun | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

<input type="checkbox"/>	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

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

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

Depois de terminar

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

Solucionar problemas de dados de objetos perdidos e ausentes

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

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

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

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

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

No caso de perda de dados de objetos sem cópias, não há solução de recuperação. No entanto, você deve redefinir o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos.

Informações relacionadas

[Investigue objetos perdidos](#)

[Repor contagens de objetos perdidas e em falta](#)

Investigue objetos perdidos

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

O que você vai precisar

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

Sobre esta tarefa

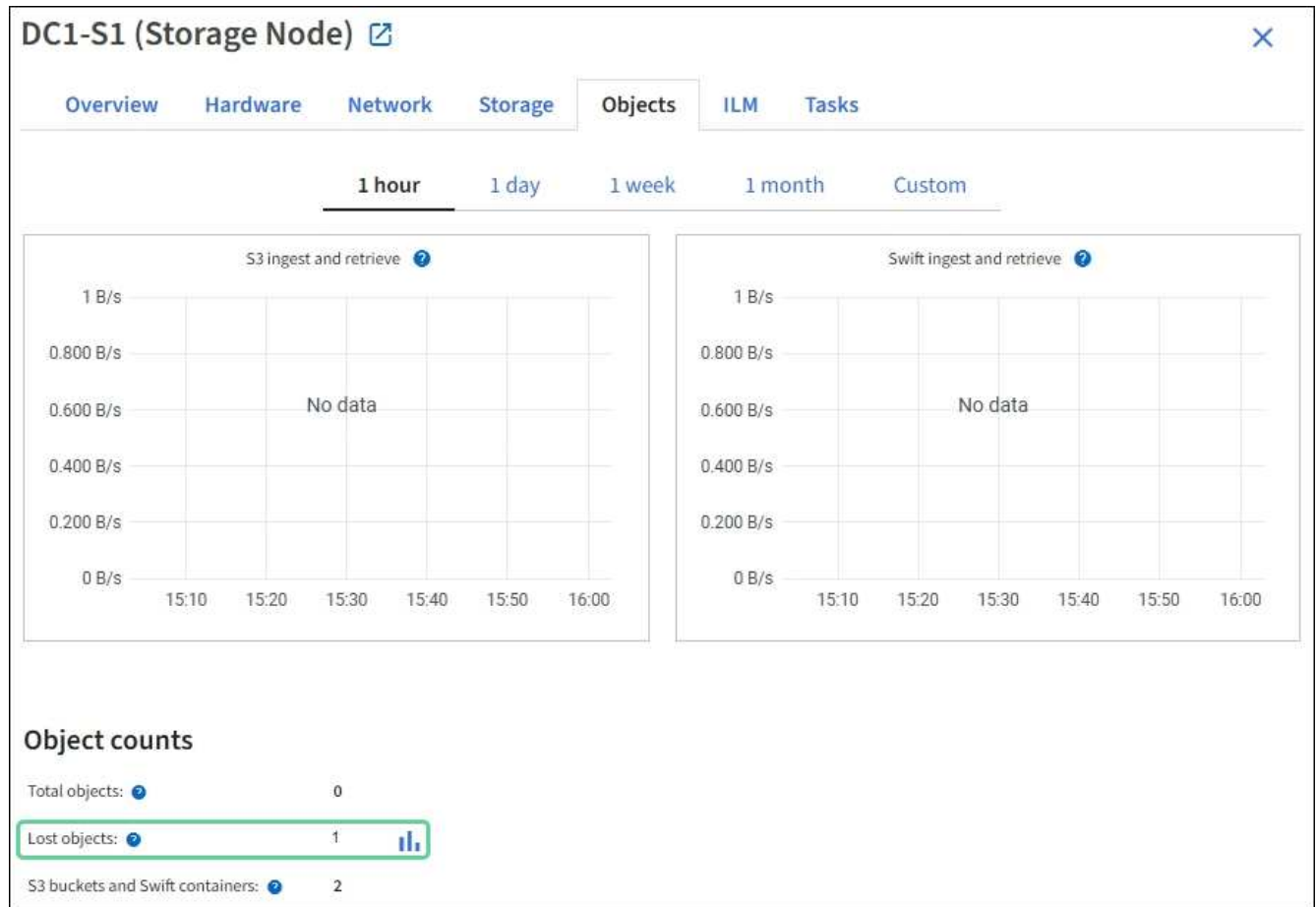
O alerta **objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

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

Passos

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

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



4. A partir de um nó Admin, acesse o log de auditoria para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **objetos perdidos**:
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
 - b. Mude para o diretório onde os logs de auditoria estão localizados. Introduza: `cd /var/local/audit/export/`
 - c. Use `grep` para extrair as mensagens de auditoria OLST (Object Lost). Introduza: `grep OLST audit_file_name`
 - d. Observe o valor UUID incluído na mensagem.

```

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

```

5. Use o `ObjectByUUID` comando para encontrar o objeto pelo seu identificador (UUID) e, em seguida, determinar se os dados estão em risco.

- a. Telnet para localhost 1402 para acessar o console LDR.
- b. Introduza: `/proc/OBRP/ObjectByUUID UUID_value`

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

```

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

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

```

```

        "ITME": "1581534970983000"
    },
    "CMSM": {
        "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
        "LOCC": "us-east-1"
    }
},
"CLCO\ (Locations\)": \[
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12448208",
        "VOLI\ (Volume ID\)": "3222345473",
        "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.880569"
    },
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12288733",
        "VOLI\ (Volume ID\)": "3222345984",
        "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.934425"
    }
]
}

```

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

```

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

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

```

a. Revise a saída de `/proc/OBRP/ObjectByUUID` e tome a ação apropriada:

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

Informações relacionadas

[Rever registros de auditoria](#)

Procure e restaure objetos potencialmente perdidos

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

O que você vai precisar

- Você deve ter o UUID de qualquer objeto perdido, conforme identificado em "investigando objetos perdidos".
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Você pode seguir este procedimento para procurar cópias replicadas do objeto perdido em outro lugar na

grade. Na maioria dos casos, o objeto perdido não será encontrado. No entanto, em alguns casos, você pode encontrar e restaurar um objeto replicado perdido se você executar uma ação de prompt.



Contacte o suporte técnico para obter assistência com este procedimento.

Passos

1. A partir de um nó Admin, procure os logs de auditoria para possíveis localizações de objetos:
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
 - b. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/audit/export/`
 - c. Use o `grep` para extrair as mensagens de auditoria associadas ao objeto potencialmente perdido e enviá-las para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

Por exemplo:

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

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

Por exemplo:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

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

```
[AUDT:\[NOID\ (UI32\) :12448208\] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP (FC32) :CLDI]
[PCLD\ (CSTR\) : "/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :
1581535134379225] [ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CL
SM]
[ATID (UI64) :7086871083190743409]]
```

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

Se presente, o valor de PCLD é o caminho completo no disco para a cópia de objeto replicado em

falta. O valor de NOID é o id do nó do LDR onde uma cópia do objeto pode ser encontrada.

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

f. Localize o nó de armazenamento para este ID de nó LDR.

Há duas maneiras de usar o ID do nó para localizar o nó de storage:

- No Gerenciador de Grade, selecione **support Tools Grid topology**. Em seguida, selecione **Data Center Storage Node LDR**. O ID do nó LDR está na tabela informações do nó. Reveja as informações de cada nó de armazenamento até encontrar o que hospeda este LDR.
- Baixe e descompacte o Pacote de recuperação para a grade. Existe um diretório `_docs` no REFERIDO pacote. Se você abrir o arquivo `index.html`, o Resumo de servidores mostrará todas as IDs de nó para todos os nós de grade.

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

a. Faça login no nó da grade:

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

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

1. Determine se o caminho do arquivo para o objeto existe.

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

Por exemplo, digite:

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

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

- Se o caminho do objeto não for encontrado, o objeto é perdido e não pode ser restaurado usando este procedimento. Entre em Contato com o suporte técnico.
- Se o caminho do objeto for encontrado, continue com a [Restaure o objeto para o StorageGRID](#) etapa . Você pode tentar restaurar o objeto encontrado de volta para o StorageGRID.
 - a. `[[restore_the_object_to_StorageGRID 3]]`se o caminho do objeto foi encontrado, tente restaurar o objeto para StorageGRID:
 - i. No mesmo nó de storage, altere a propriedade do arquivo de objeto para que ele possa ser gerenciado pelo StorageGRID. Introduza: `chown ldr-user:bycast 'file_path_of_object'`
 - ii. Telnet para localhost 1402 para acessar o console LDR. Introduza: `telnet 0 1402`
 - iii. Introduza: `cd /proc/STOR`
 - iv. Introduza: `Object_Found 'file_path_of_object'`

Por exemplo, digite:

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

A emissão do `Object_Found` comando notifica a grade da localização do objeto. Ele também aciona a política ILM ativa, que faz cópias adicionais conforme especificado na política.

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

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

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

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Avance para o passo [Verifique se foram criados novos locais](#)

- v. se o objeto foi restaurado com sucesso para o StorageGRID, verifique se novos locais foram criados.
 - A. Introduza: `cd /proc/OBRP`
 - B. Introduza: `ObjectByUUID UUID_value`

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

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

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
```

```

"BASE(Protocol metadata)": {
  "PAWS(S3 protocol version)": "2",
  "ACCT(S3 account ID)": "44084621669730638018",
  "*ctp(HTTP content MIME type)": "binary/octet-stream"
},
"BYCB(System metadata)": {
  "CSIZ(Plaintext object size)": "5242880",
  "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
  "BSIZ(Content block size)": "5252084",
  "CVER(Content block version)": "196612",
  "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
  "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
  "ITME": "1581534970983000"
},
"CMSM": {
  "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
},
"AWS3": {
  "LOCC": "us-east-1"
}
},
"CLCO\ (Locations\)": \[
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12448208",
    "VOLI\ (Volume ID\)": "3222345473",
    "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
    "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.880569"
  },
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12288733",
    "VOLI\ (Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.934425"
  }
]
}

```

1. Saia da consola LDR. Introduza: exit

- a. Em um nó Admin, pesquise os logs de auditoria para a mensagem de auditoria ORLM para este objeto para confirmar que o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme necessário.
2. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
3. Mude para o diretório onde os logs de auditoria estão localizados: `cd /var/local/audit/export/`
4. Use `grep` para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída. Introduza: `grep uuid-valueaudit_file_name > output_file_name`

Por exemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

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

Por exemplo:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

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

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

6. Localize o campo `LOCS` na mensagem de auditoria.

Se presente, o valor de `CLDI` em `LOCS` é o ID do nó e o ID do volume onde uma cópia de objeto foi criada. Esta mensagem mostra que o ILM foi aplicado e que duas cópias de objeto foram criadas em dois locais na grade. . Redefina a contagem de objetos perdidos no Gerenciador de Grade.

Informações relacionadas

[Investigue objetos perdidos](#)

[Repor contagens de objetos perdidas e em falta](#)

[Rever registros de auditoria](#)

Repor contagens de objetos perdidas e em falta

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

O que você vai precisar

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

Sobre esta tarefa

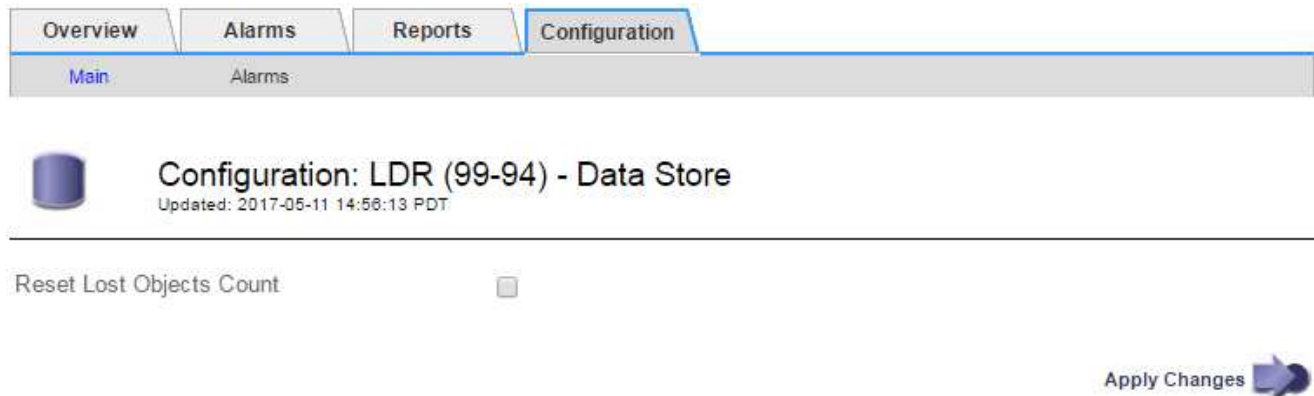
Você pode redefinir o contador de objetos perdidos a partir de uma das seguintes páginas:

- **SUPORTE Ferramentas topologia de grade *Site Storage Node* LDR Data Store Visão geral Main**
- **SUPORTE Ferramentas topologia de grade *Site Storage Node* DDS Data Store Visão geral Principal**

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

Passos

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



4. Clique em **aplicar alterações**.

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

5. Opcionalmente, redefina outros valores de atributo relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.
 - a. Selecione ***Site Storage Node* LDR Codificação de apagamento Configuração**.
 - b. Selecione **Redefinir leituras de contagem de falhas** e **Redefinir cópias corrompidas detetadas**

contagem.

- c. Clique em **aplicar alterações**.
- d. Selecione **Site Storage Node LDR Verificação Configuração**.
- e. Selecione **Redefinir contagem de objetos ausentes** e **Redefinir contagem de objetos corrompidos**.
- f. Se você tiver certeza de que objetos em quarentena não são necessários, selecione **Excluir objetos em quarentena**.

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

- g. Clique em **aplicar alterações**.

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

Solucionar problemas do alerta de armazenamento de dados de objetos baixos

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

O que você vai precisar

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

Sobre esta tarefa

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

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

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

Nesta condição:

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

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

Passos

1. Selecione **ALERTAS current**.

A página Alertas é exibida.

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



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

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

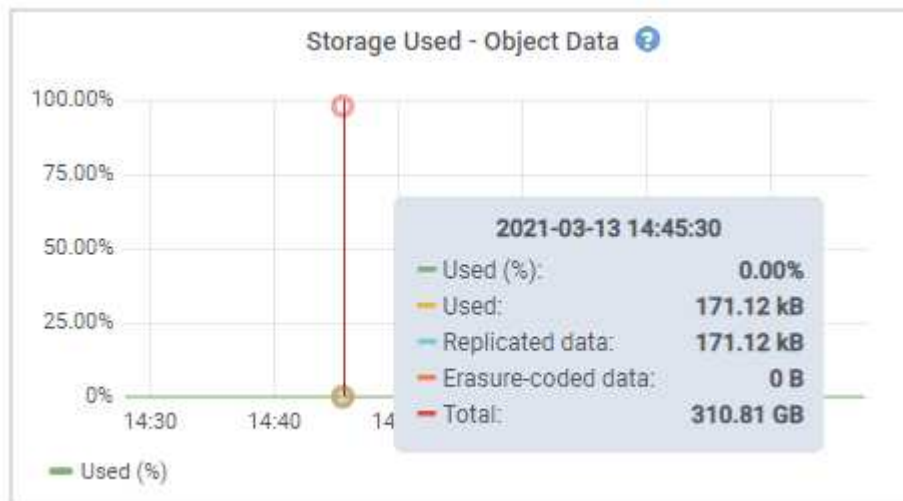
- Tempo acionado
- O nome do site e do nó
- Os valores atuais das métricas para este alerta

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

5. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados do objeto).

São apresentados os seguintes valores:

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



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

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

7. Assim que possível, execute um procedimento de expansão para adicionar capacidade de armazenamento.

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



Para gerenciar um nó de storage completo, consulte as instruções de administração do StorageGRID.

Informações relacionadas

[Soluçione o problema do alarme de Status de armazenamento \(SSTS\)](#)

[Expanda sua grade](#)

[Administrar o StorageGRID](#)

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

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

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

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

- Seu sistema está próximo da capacidade e não poderá aceitar novos dados se forem aplicadas marcas de água otimizadas. Neste caso, o StorageGRID não alterará as configurações de marca d'água.
- Você definiu anteriormente qualquer uma das marcas d'água do volume de armazenamento para um valor personalizado. O StorageGRID não substituirá as configurações personalizadas de marca d'água com valores otimizados. No entanto, o StorageGRID pode acionar o alerta de substituição de marca d'água **baixa somente leitura** se o valor personalizado para a marca d'água de volume de armazenamento Soft somente leitura for muito pequeno.

Entenda o alerta

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

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

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

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

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

Resolva o alerta

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

O que você vai precisar

- Concluiu a atualização para o StorageGRID 11,6.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

Sobre esta tarefa

Você pode resolver o alerta * baixa substituição de marca d'água somente leitura * atualizando as configurações personalizadas de marca d'água para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem próximos do cheio ou se você tiver requisitos especiais de ILM, primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados de objeto para toda a grade

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

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
⚠ DC1-SN1	Storage Node	71%	3%	30%
⚠ DC1-SN2	Storage Node	25%	3%	42%
⚠ DC1-SN3	Storage Node	63%	3%	42%
⚠ DC1-SN4	Storage Node	65%	3%	41%

4. Se nenhum dos nós de armazenamento estiver próximo da totalidade (por exemplo, todos os valores **dados de objeto usados** forem inferiores a 80%), você poderá começar a usar as configurações de substituição. Vá para [Use marcas de água otimizadas](#).



Existem algumas exceções a esta regra geral. Por exemplo, se as regras do ILM usarem comportamento de ingestão estrito ou se pools de armazenamento específicos estiverem próximos de cheio, primeiro execute as etapas no [Ver marcas de água de armazenamento otimizadas](#) e [Determine se você pode usar marcas de água otimizadas](#) no .

5. Se mais um nó de storage estiver próximo ao completo, execute as etapas em [Ver marcas de água de armazenamento otimizadas](#) e [Determine se você pode usar marcas de água otimizadas](#).

Ver marcas de água de armazenamento otimizadas

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

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

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

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

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

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

Determine se você pode usar marcas de água otimizadas

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

Caso contrário, [expanda sua grade](#) logo que possível. Adicione volumes de storage a um nó existente ou adicione novos nós de storage. Em seguida, acesse [Use marcas de água otimizadas](#) para atualizar as definições da marca de água.

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



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

Use marcas de água otimizadas

1. Vá para **CONFIGURATION System Storage options**.
2. Selecione **Configuração** no menu Opções de armazenamento.
3. Altere todas as três substituições do Watermark para 0.
4. Selecione **aplicar alterações**.

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

Storage Options

- Overview
- Configuration

Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

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

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

O que você vai precisar

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

Sobre esta tarefa

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



Storage Options Overview

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

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

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

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

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

Passos

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

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

Overview
Alarms
Reports
Configuration

Main
History

Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

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

Apply Changes

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



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

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

Overview: LDR (:DC1-S1-101-193) - Storage
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired: Online
Storage State - Current: Read-only
Storage Status: Insufficient Free Space

Utilization

Total Space:	164 GB
Total Usable Space:	19.6 GB
Total Usable Space (Percent):	11.937 %
Total Data:	139 GB
Total Data (Percent):	84.567 %

Replication

Block Reads:	0
Block Writes:	2,279,881
Objects Retrieved:	0
Objects Committed:	88,882
Objects Deleted:	16
Delete Service State:	Enabled

Object Store Volumes

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

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

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

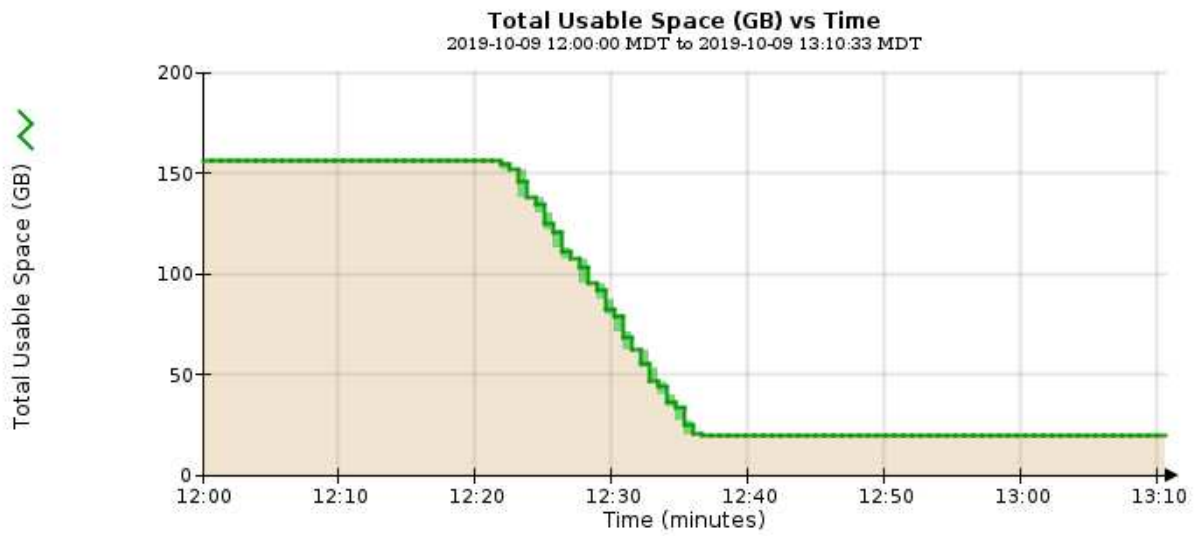
Neste exemplo, o espaço utilizável total caiu de cerca de 155 GB em 12:00 para 20 GB em 12:35, o que corresponde ao momento em que o alarme SSTS foi acionado.



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33

YYYY/MM/DD HH:MM:SS




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

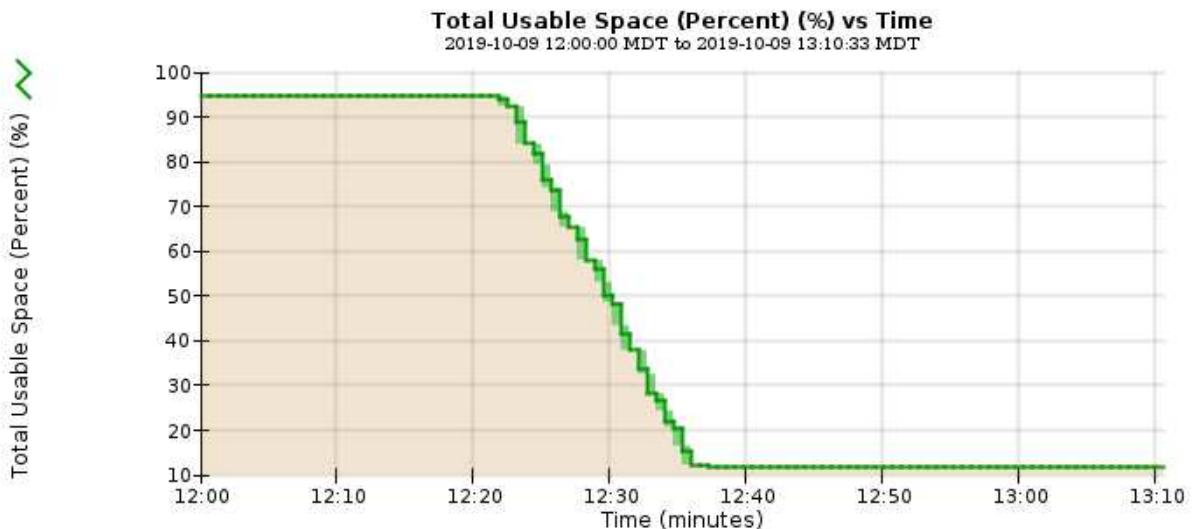
Neste exemplo, o espaço utilizável total caiu de 95% para pouco mais de 10%, aproximadamente ao mesmo tempo.

Overview | Alarms | **Reports** | Configuration

Charts | Text

 Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute: Total Usable Space (Percent) Vertical Scaling: Start Date: 2019/10/09 12:00:00
 Quick Query: Custom Query Update Raw Data: End Date: 2019/10/09 13:10:33



6. Conforme necessário, adicione a capacidade de armazenamento por [Expansão do sistema StorageGRID](#).

Para obter procedimentos sobre como gerenciar um nó de storage completo, consulte [Instruções para administrar o StorageGRID](#).

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

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

Sobre esta tarefa

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

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

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

Para obter informações adicionais sobre a solução de problemas dos serviços da plataforma, consulte o [Instruções para administrar o StorageGRID](#). Talvez seja necessário [Acesse o localitário do Gerenciador do Localitário](#) depurar um erro de serviço de plataforma.

Passos

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

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

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

Solucionar problemas de metadados

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

Solucionar problemas do alerta de armazenamento de metadados baixos

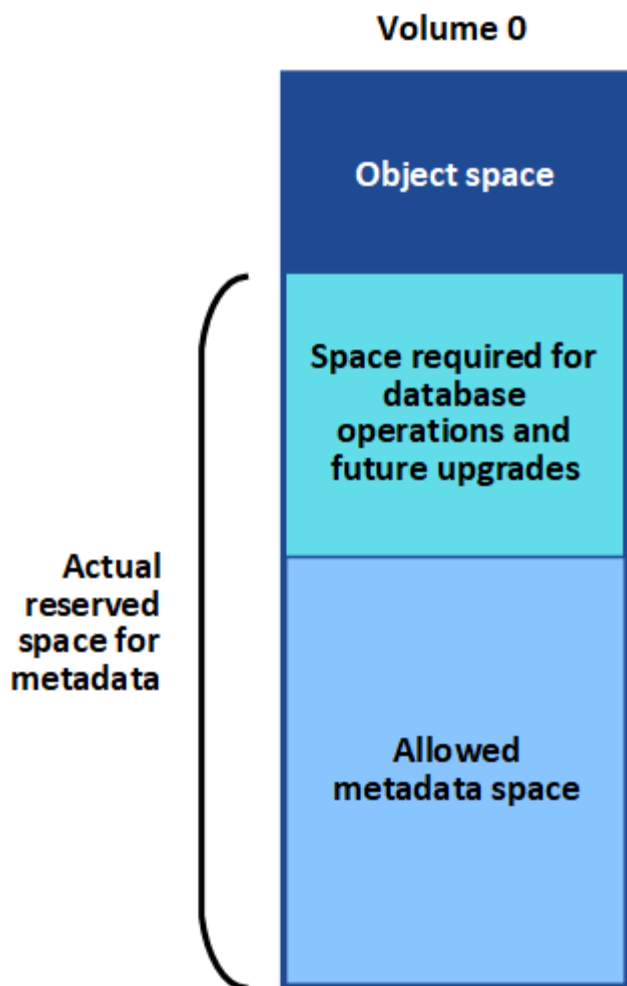
Se o alerta **armazenamento de metadados baixo** for acionado, você deverá adicionar novos nós de armazenamento.

O que você vai precisar

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

Sobre esta tarefa

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



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

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

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

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



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

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

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

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

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

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



Se o tamanho do volume 0 for menor do que a opção de armazenamento de espaço reservado de metadados (por exemplo, em um ambiente não-produção), o cálculo do alerta **armazenamento de metadados baixo** pode ser impreciso.

Passos

1. Selecione **ALERTAS current**.
2. Na tabela de alertas, expanda o grupo de alertas **armazenamento de metadados baixo**, se necessário, e selecione o alerta específico que deseja exibir.
3. Reveja os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **armazenamento de metadados baixo** tiver sido acionado, execute uma expansão para adicionar nós de armazenamento imediatamente.



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

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

Solucionar problemas do alarme Serviços: Status - Cassandra (SVST)

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

O que você vai precisar

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

Sobre esta tarefa

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

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



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

Passos

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

Este exemplo mostra que o alarme SVST foi acionado.

Severity Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

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

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC2-S1) - Services

Updated: 2017-03-30 09:53:53 MDT

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

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



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

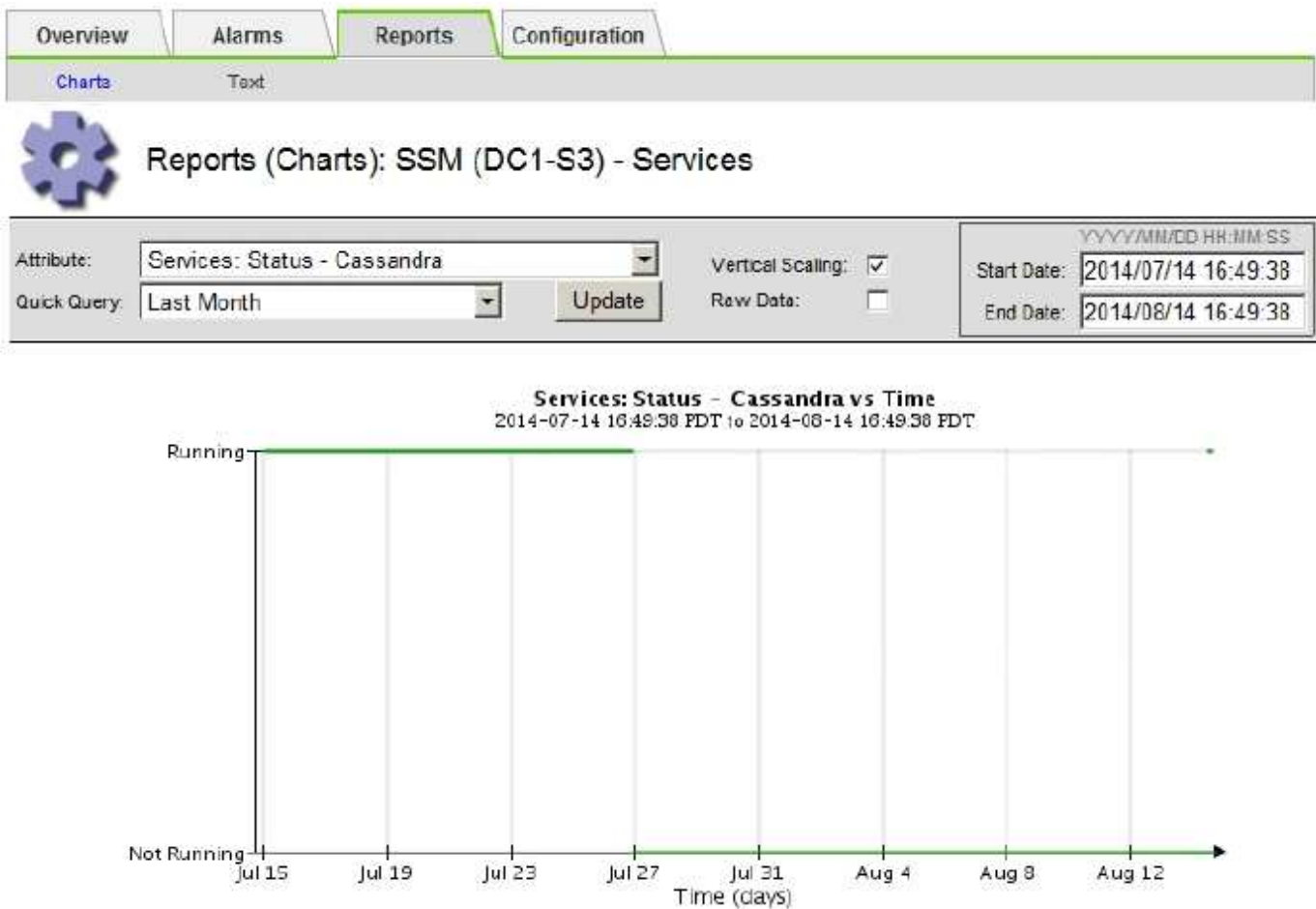
Você pode determinar por quanto tempo o Cassandra ficou para baixo, traçando-o ou revisando o arquivo `servermanager.log`.

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

d. Clique em **Atualizar**.

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

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



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

a. Faça login no nó da grade:

i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro. Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

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

O conteúdo do arquivo `servermanager.log` é exibido.

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


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

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

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

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

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

- c. Entre em Contato com o suporte técnico se os alarmes não forem apagados após a reconstrução do Cassandra.

Resolução de problemas de erros de memória sem Cassandra (alarme SMTT)

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

Sobre esta tarefa

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

Passos

1. Para visualizar o evento, selecione **support Tools Grid topology Configuration**.
2. Verifique se a contagem de erros de memória do Cassandra Heap é 1 ou superior.

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

3. Vá para `/var/local/core/`, compacte o `Cassandra.hprof` arquivo e envie-o para o suporte técnico.
4. Faça um backup do `Cassandra.hprof` arquivo e exclua-o do `/var/local/core/` directory.

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

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



Para redefinir contagens de eventos, você deve ter a permissão Configuração de Página de topologia de Grade.

Solucionar erros de certificado

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

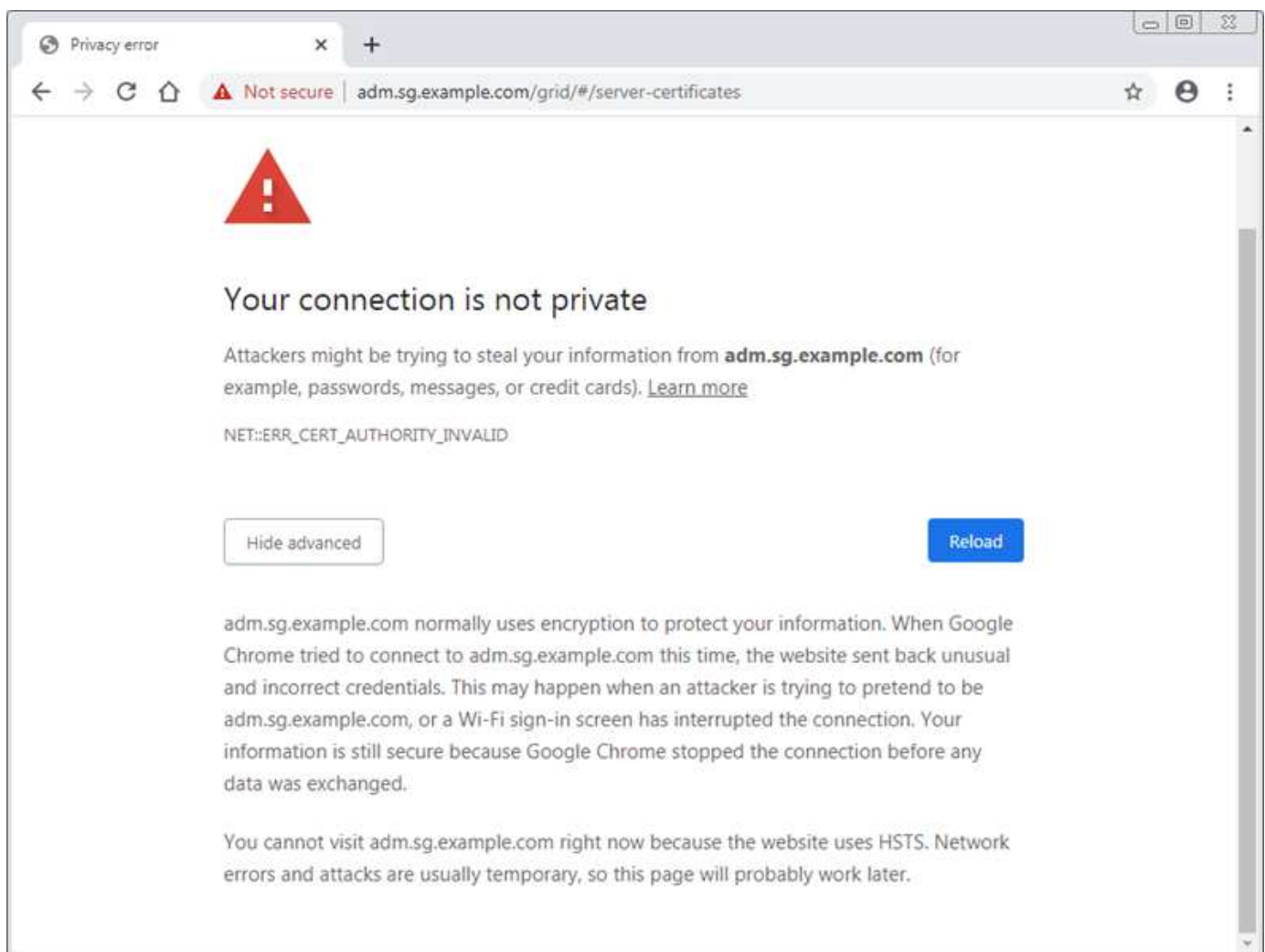
Sobre esta tarefa

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

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

- O certificado de interface de gerenciamento personalizado expira.
- Você reverte de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão.

O exemplo a seguir mostra um erro de certificado quando o certificado de interface de gerenciamento personalizado expirou:



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

Quando você estiver usando certificados de cliente para integração externa do Prometheus, erros de certificado podem ser causados pelo certificado de interface de gerenciamento do StorageGRID ou por

certificados de cliente. O alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando um certificado de cliente está prestes a expirar.

Passos

Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado: . Selecione **CONFIGURATION Security Certificates** e, em seguida [selecione a guia certificado apropriado](#), .

1. Verifique o período de validade do certificado. Alguns navegadores web e clientes S3 ou Swift não aceitam certificados com um período de validade superior a 398 dias.
2. Se o certificado tiver expirado ou expirar em breve, carregue ou gere um novo certificado.
 - Para obter um certificado de servidor, consulte as etapas [Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário](#)do .
 - Para obter um certificado de cliente, consulte as etapas [configurando um certificado de cliente](#)do .
3. Para erros de certificado de servidor, tente uma ou ambas as opções a seguir:
 - Certifique-se de que o nome alternativo do assunto (SAN) do certificado esteja preenchido e que a SAN corresponda ao endereço IP ou ao nome do host do nó ao qual você está se conectando.
 - Se você estiver tentando se conectar ao StorageGRID usando um nome de domínio:
 - i. Insira o endereço IP do nó Admin em vez do nome de domínio para ignorar o erro de conexão e acessar o Gerenciador de Grade.
 - ii. No Gerenciador de Grade, selecione **CONFIGURATION Security Certificates** e, em seguida [selecione a guia certificado apropriado](#), instale um novo certificado personalizado ou continue com o certificado padrão.
 - iii. Nas instruções de administração do StorageGRID, consulte as etapas [Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário](#)do .

Solucionar problemas de nó de administração e interface do usuário

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

Solucionar erros de logon

Se ocorrer um erro ao iniciar sessão num nó de administração do StorageGRID, o sistema poderá ter um problema com a configuração da federação de identidade, um problema de rede ou hardware, um problema com os serviços do nó de administração ou um problema com o banco de dados Cassandra nos nós de armazenamento conectados.

O que você vai precisar

- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

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

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start...`

- Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.
- Unable to communicate with server. Reloading page...

Passos

1. Aguarde 10 minutos e tente iniciar sessão novamente.

Se o erro não for resolvido automaticamente, vá para a próxima etapa.

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

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



Se o SSO estiver ativado, você não poderá fazer login usando uma porta restrita. Tem de utilizar a porta 443.

5. Determine se a conta que você está usando pertence a um usuário federado.

Se a conta de usuário federada não estiver funcionando, tente fazer login no Gerenciador de Grade como um usuário local, como root.

- Se o utilizador local puder iniciar sessão:
 - i. Reveja todos os alarmes apresentados.
 - ii. Selecione **CONFIGURATION Access Control Identity Federation**.
 - iii. Clique em **Test Connection** para validar as configurações de conexão para o servidor LDAP.
 - iv. Se o teste falhar, resolva quaisquer erros de configuração.
 - Se o usuário local não conseguir fazer login e tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.
6. Use o Secure Shell (ssh) para fazer login no Admin Node:
 - a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

7. Veja o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços de api nms, mi, nginx e mgmt estejam todos em execução.

A saída é atualizada imediatamente se o status de um serviço mudar.

```
$ storagegrid-status
Host Name                99-211
IP Address                10.96.99.211
Operating System Kernel  4.19.0                 Verified
Operating System Environment Debian 10.1             Verified
StorageGRID Webscale Release 11.4.0                 Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine          5.5.9999+default      Running
Network Monitoring       11.4.0                 Running
Time Synchronization     1:4.2.8p10+dfsg      Running
ams                       11.4.0                 Running
cmn                       11.4.0                 Running
nms                       11.4.0                 Running
ssm                       11.4.0                 Running
mi                        11.4.0                 Running
dynip                    11.4.0                 Running
nginx                    1.10.3                 Running
tomcat                   9.0.27                 Running
grafana                  6.4.3                 Running
mgmt api                 11.4.0                 Running
prometheus               11.4.0                 Running
persistence              11.4.0                 Running
ade exporter             11.4.0                 Running
alertmanager             11.4.0                 Running
attrDownPurge            11.4.0                 Running
attrDownSamp1            11.4.0                 Running
attrDownSamp2            11.4.0                 Running
node exporter            0.17.0+ds              Running
sg snmp agent            11.4.0                 Running
```

8. Confirme se o serviço nginx-gw está em execução # `service nginx-gw status`

9. Use Lumberjack para coletar logs: # `/usr/local/sbin/lumberjack.rb`

Se a autenticação com falha aconteceu no passado, você pode usar as opções de script `--start` e `--end` Lumberjack para especificar o intervalo de tempo apropriado. Use `lumberjack -h` para obter detalhes sobre essas opções.

A saída para o terminal indica onde o arquivo de log foi copiado.

10. Rever os seguintes logs:

- `/var/local/log/bycast.log`

- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Se você não conseguir identificar nenhum problema com o nó Admin, emita um dos seguintes comandos para determinar os endereços IP dos três nós de armazenamento que executam o serviço ADC em seu site. Em geral, esses são os primeiros três nós de storage instalados no local.

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

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

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

12. A partir do nó Admin, efetue login em cada um dos nós de armazenamento ADC, usando os endereços IP identificados.
- Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - Digite o seguinte comando para mudar para root: `su -`
 - Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

13. Veja o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços `idnt`, `acct`, `nginx` e `cassandra` estejam todos em execução.

14. Repita as etapas [Use Lumberjack para coletar logs](#) e [Rever registros](#) para revisar os logs nos nós de storage.

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

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

Solucionar problemas de interface do usuário

Você pode ver problemas com o Gerenciador de Grade ou o Gerenciador do Locatário após atualizar para uma nova versão do software StorageGRID.

A interface Web não responde como esperado

O Gerenciador de Grade ou o Gerente do Locatário podem não responder como esperado depois que o software StorageGRID for atualizado.

Se você tiver problemas com a interface da Web:

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



O suporte do navegador foi alterado para o StorageGRID 11,5. Confirme que está a utilizar uma versão suportada.

- Limpe o cache do navegador da Web.

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

Verifique o status de um Admin Node indisponível

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

O que você vai precisar

Você deve ter permissões de acesso específicas.

Passos

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



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

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

Operating System: Linux
3.16.0-4-amd64

Services

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

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

Informações relacionadas

[Administrar o StorageGRID](#)

Solucionar problemas de rede, hardware e plataforma

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

Solucione os erros "422: Entidade não processável"

O erro 422: Entidade não processável pode ocorrer em várias circunstâncias. Verifique a mensagem de erro para determinar o que causou o problema.

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

Mensagem de erro	Causa raiz e ação corretiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	<p>Esta mensagem pode ocorrer se você selecionar a opção não usar TLS para Segurança da camada de Transporte (TLS) ao configurar a federação de identidade usando o Windows active Directory (AD).</p> <p>O uso da opção não usar TLS não é suportado para uso com servidores AD que imponham a assinatura LDAP. Você deve selecionar a opção usar STARTTLS ou a opção usar LDAPS para TLS.</p>
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	<p>Essa mensagem será exibida se você tentar usar uma cifra não suportada para fazer uma conexão TLS (Transport Layer Security) do StorageGRID para um sistema externo usado para identificar pools de federação ou armazenamento em nuvem.</p> <p>Verifique as cifras que são oferecidas pelo sistema externo. O sistema deve usar uma das cifras suportadas pelo StorageGRID para conexões TLS de saída, como mostrado nas instruções de administração do StorageGRID.</p>

Informações relacionadas

[Administrar o StorageGRID](#)

solucione o alerta de incompatibilidade da MTU da rede de Grade

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

Sobre esta tarefa

As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 são

configuradas para quadros jumbo. Uma incompatibilidade de tamanho da MTU superior a 1000 pode causar problemas de desempenho da rede.

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
 - Use a consulta fornecida no Gerenciador de Grade.
 - Navegue para *primary Admin Node IP address/metrics/graph* e insira a seguinte consulta:
`node_network_mtu_bytes{interface='eth0'}`
2. Modifique as configurações de MTU conforme necessário para garantir que elas sejam as mesmas para a interface de rede de Grade (eth0) em todos os nós.
 - Para os nós do dispositivo, consulte as instruções de instalação e manutenção do seu dispositivo.
 - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

Exemplo: `change-ip.py -n node 1500 grid admin`

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

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

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

+

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

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

[SG6000 dispositivos de armazenamento](#)

Solucionar problemas do alarme Network Receive Error (NRER)

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

Sobre esta tarefa

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

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

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas do alarme NRER, dada a configuração da rede.

- Se o erro for causado por incompatibilidade de FEC, execute as seguintes etapas:

Nota: Estas etapas são aplicáveis apenas para erros NRER causados por incompatibilidade FEC em aparelhos StorageGRID.

- i. Verifique o status do FEC da porta no switch conectado ao seu dispositivo StorageGRID.
- ii. Verifique a integridade física dos cabos do aparelho ao interruptor.
- iii. Se pretender alterar as definições do FEC para tentar resolver o alarme NRER, certifique-se primeiro de que o aparelho está configurado para o modo **Auto** na página Configuração de ligação do Instalador de dispositivos StorageGRID (consulte as instruções de instalação e manutenção do seu aparelho). Em seguida, altere as configurações do FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações FEC para corresponder, se possível.

(Não é possível configurar as definições FEC nos dispositivos StorageGRID. Em vez disso, os aparelhos tentam descobrir e espelhar as configurações FEC nas portas do switch às quais estão conectados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC poderão não conseguir negociar uma configuração FEC comum. Sem uma configuração comum de FEC, a rede voltará ao modo "no-FEC". Quando o FEC não está ativado, as conexões são mais suscetíveis a erros causados por ruído elétrico.)

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

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

O tamanho da MTU configurado no nó pode ser menor do que a configuração na porta do switch à qual o nó está conectado. Se um nó StorageGRID receber um quadro Ethernet maior que o MTU, o que é possível com esta configuração, o alarme NRER pode ser comunicado. Se você acredita que isso

está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede da StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo dos seus objetivos ou requisitos de MTU de ponta a ponta.



Para obter o melhor desempenho de rede, todos os nós devem ser configurados com valores MTU semelhantes em suas interfaces de rede de Grade. O alerta **incompatibilidade de MTU da rede de Grade** é acionado se houver uma diferença significativa nas configurações de MTU para a rede de Grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede.



Para alterar a definição MTU, consulte o guia de instalação e manutenção do seu aparelho.

- Se o erro for causado por altas taxas de erro de link, execute as seguintes etapas:
 - i. Ative o FEC, se ainda não estiver ativado.
 - ii. Verifique se o cabeamento de rede é de boa qualidade e não está danificado ou conectado incorretamente.
 - iii. Se os cabos parecerem não ser o problema, contacte o suporte técnico.



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

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

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

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

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

Informações relacionadas

[Solucione o alerta de incompatibilidade da MTU da rede de Grade](#)

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

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG5600 dispositivos de armazenamento](#)

[Aparelhos de serviços SG100 e SG1000](#)

Solucionar erros de sincronização de tempo

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

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



Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

Informações relacionadas

[Recuperar e manter](#)

Linux: Problemas de conectividade de rede

Você pode ver problemas com a conectividade de rede para nós de grade StorageGRID hospedados em hosts Linux.

Clonagem de endereços MAC

Em alguns casos, os problemas de rede podem ser resolvidos usando a clonagem de endereços MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereços MAC para cada uma de suas redes como "verdadeiro" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do contentor StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções no guia de instalação da sua plataforma.



Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contentor StorageGRID pode fazer com que o sistema operacional do host se torne inacessível se o modo promíscuo não tiver sido ativado no hypervisor.

Para obter mais informações sobre como ativar a clonagem MAC, consulte as instruções no guia de instalação da sua plataforma.

Modo promíscuo

Se você não quiser usar a clonagem de endereços MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes dos atribuídos pelo hypervisor, verifique se as propriedades de segurança nos níveis de switch virtual e grupo de portas estão definidas como **Accept** para modo promíscuo, alterações de endereço MAC e transmissões forjadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

Linux: O status do nó é "órfão"

Um nó Linux em um estado órfão geralmente indica que o serviço StorageGRID ou o daemon de nó StorageGRID que controla o contentor do nó morreram inesperadamente.

Sobre esta tarefa

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

- Verifique os logs para ver se há erros e mensagens.

- Tente iniciar o nó novamente.
- Se necessário, use comandos do mecanismo do contentor para parar o contentor do nó existente.
- Reinicie o nó.

Passos

1. Verifique os logs do serviço daemon e do nó órfão para ver se há erros óbvios ou mensagens sobre sair inesperadamente.
2. Faça login no host como root ou usando uma conta com permissão sudo.
3. Tente iniciar o nó novamente executando o seguinte comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se o nó estiver órfão, a resposta será

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

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

Para `seconds`, introduza o número de segundos que pretende aguardar que o recipiente pare (normalmente, 15 minutos ou menos). Por exemplo:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Reinicie o nó: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Solucione problemas de suporte ao IPv6

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

Sobre esta tarefa

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

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

DC1-S2 (Storage Node)

Overview Hardware Network Storage Objects ILM Tasks

Node information

Name: DC1-S2
 Type: Storage Node
 ID: 352bd978-ff3e-45c5-aac1-24c7278206fa
 Connection state: ✔ Connected
 Storage used: Object data 0%
 Object metadata 0%
 Software version: 11.6.0 (build 20210924.1557.00a5eb9)
 IP addresses: 172.16.1.227 - eth0 (Grid Network)
 10.224.1.227 - eth1 (Admin Network)
[Hide additional IP addresses](#)

Interface	IP address
eth0 (Grid Network)	172.16.1.227
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532

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

Se o endereço IPv6 não for exibido e o nó estiver instalado em um host Linux, siga estas etapas para habilitar o suporte a IPv6 no kernel.

Passos

1. Faça login no host como root ou usando uma conta com permissão sudo.
2. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Se o resultado não for 0, consulte a documentação do sistema operacional para alterar `sysctl` as configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Insira o contentor do nó StorageGRID: `storagegrid node enter node-name`

4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Se o resultado não for 1, este procedimento não se aplica. Entre em Contato com o suporte técnico.

5. Saia do recipiente: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite o seguinte arquivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localize as duas linhas a seguir e remova as tags de comentário. Em seguida, salve e feche o arquivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Execute estes comandos para reiniciar o contentor StorageGRID:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Solucionar problemas de um servidor syslog externo

A tabela a seguir descreve as mensagens de erro do servidor syslog externo e lista as ações corretivas.

Mensagem de erro	Descrição e ações recomendadas
Não é possível resolver o nome do host	<p>O FQDN inserido para o servidor syslog não pôde ser resolvido para um endereço IP.</p> <ol style="list-style-type: none"> 1. Verifique o nome do host que você inseriu. Se você inseriu um endereço IP, verifique se ele é um endereço IP válido na notação W.X.Y.Z ("decimal pontilhado"). 2. Verifique se os servidores DNS estão configurados corretamente. 3. Confirme se cada nó pode acessar os endereços IP do servidor DNS.
Ligação recusada	<p>Uma conexão TCP ou TLS ao servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS para o host, ou um firewall pode estar bloqueando o acesso.</p> <ol style="list-style-type: none"> 1. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. 2. Confirme se o host do serviço syslog está executando um daemon syslog que está escutando na porta especificada. 3. Confirme se um firewall não está bloqueando o acesso a conexões TCP/TLS dos nós para o IP e a porta do servidor syslog.
Rede inacessível	<p>O servidor syslog não está em uma sub-rede conetada diretamente. Um roteador retornou uma mensagem de falha ICMP para indicar que não foi possível encaminhar as mensagens de teste dos nós listados para o servidor syslog.</p> <ol style="list-style-type: none"> 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog através da interface de rede e gateway esperados (Grid, Admin ou Client).
Host inalcançável	<p>O servidor syslog está em uma sub-rede conetada diretamente (sub-rede usada pelos nós listados para seus endereços IP de Grade, Admin ou Cliente). Os nós tentaram enviar mensagens de teste, mas não receberam respostas a solicitações ARP para o endereço MAC do servidor syslog.</p> <ol style="list-style-type: none"> 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Verifique se o host que executa o serviço syslog está ativo.

Mensagem de erro	Descrição e ações recomendadas
Tempo de ligação esgotado	<p>Uma tentativa de conexão TCP/TLS foi feita, mas nenhuma resposta foi recebida do servidor syslog por um longo tempo. Pode haver uma configuração incorreta de roteamento ou um firewall pode estar deixando cair o tráfego sem enviar qualquer resposta (uma configuração comum).</p> <ol style="list-style-type: none"> 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes de rede de Grade, as listas de sub-redes de Admin e os gateways de rede de cliente. Confirme que estão configurados para rotear o tráfego para o servidor syslog através da interface de rede e gateway (Grid, Admin ou Client) sobre o qual você espera que o servidor syslog seja alcançado. 3. Confirme se um firewall não está bloqueando o acesso a conexões TCP/TLS dos nós listados para o IP e a porta do servidor syslog.
Conexão fechada pelo parceiro	<p>Uma conexão TCP ao servidor syslog foi estabelecida com êxito, mas foi fechada mais tarde. As razões para isso podem incluir:</p> <ul style="list-style-type: none"> • O servidor syslog pode ter sido reiniciado ou reiniciado. • O nó e o servidor syslog podem ter configurações diferentes de TCP/TLS. • Um firewall intermediário pode estar fechando conexões TCP ociosas. • Um servidor que não seja syslog escutando na porta do servidor syslog pode ter fechado a conexão. <ol style="list-style-type: none"> a. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. b. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. c. Verifique se um firewall intermediário não está configurado para fechar conexões TCP ociosas.
Erro de certificado TLS	<p>O certificado de servidor recebido do servidor syslog não era compatível com o pacote de certificados CA e o certificado de cliente fornecido.</p> <ol style="list-style-type: none"> 1. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor syslog. 2. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.

Mensagem de erro	Descrição e ações recomendadas
Reencaminhamento suspenso	<p>Os Registros do syslog não estão mais sendo encaminhados para o servidor syslog e o StorageGRID não consegue detetar o motivo.</p> <p>Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz.</p>
Sessão TLS terminada	<p>O servidor syslog encerrou a sessão TLS e o StorageGRID não consegue detetar o motivo.</p> <ol style="list-style-type: none"> 1. Revise os logs de depuração fornecidos com esse erro para tentar determinar a causa raiz. 2. Verifique se você inseriu o FQDN ou o endereço IP correto, a porta e o protocolo para o servidor syslog. 3. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 4. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor syslog. 5. Confirme se as identidades no certificado de servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Falha na consulta de resultados	<p>O nó Admin usado para configuração e teste do servidor syslog não consegue solicitar resultados de teste dos nós listados. Um ou mais nós podem estar inativos.</p> <ol style="list-style-type: none"> 1. Siga as etapas padrão de solução de problemas para garantir que os nós estejam online e que todos os serviços esperados estejam em execução. 2. Reinicie o serviço miscd nos nós listados.

Referência de alertas

A tabela a seguir lista todos os alertas padrão do StorageGRID. Conforme necessário, você pode criar regras de alerta personalizadas para se adequar à sua abordagem de gerenciamento de sistema.

Consulte as informações sobre [Métricas de Prometheus comumente usadas](#) para saber mais sobre as métricas usadas em alguns desses alertas.

Nome do alerta	Descrição e ações recomendadas
A bateria do aparelho expirou	<p>A bateria do controlador de armazenamento do aparelho expirou.</p> <ol style="list-style-type: none"> 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções do seu dispositivo de armazenamento: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.
A bateria do aparelho falhou	<p>A bateria do controlador de armazenamento do aparelho falhou.</p> <ol style="list-style-type: none"> 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções do seu dispositivo de armazenamento: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.
A bateria do aparelho não tem capacidade programada suficiente	<p>A bateria do controlador de armazenamento do aparelho não tem capacidade de aprendizagem suficiente.</p> <ol style="list-style-type: none"> 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções do seu dispositivo de armazenamento: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
A bateria do aparelho está quase a expirar	<p>A bateria do controlador de armazenamento do aparelho está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Substitua a bateria em breve. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções do seu dispositivo de armazenamento: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.
Bateria do aparelho removida	<p>A bateria do controlador de armazenamento do aparelho está em falta.</p> <ol style="list-style-type: none"> 1. Instale uma bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções do seu dispositivo de armazenamento: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.
Bateria do aparelho demasiado quente	<p>A bateria do controlador de armazenamento do aparelho está sobreaquecida.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Investigue possíveis razões para o aumento de temperatura, como uma falha da ventoinha ou do sistema de ar condicionado, ventilação e aquecimento (HVAC). 3. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Erro de comunicação do Appliance BMC	<p>A comunicação com o controlador de gestão do rodapé (BMC) foi perdida.</p> <ol style="list-style-type: none"> 1. Confirme se o BMC está a funcionar normalmente. Selecione NÓS e, em seguida, selecione a guia hardware para o nó do dispositivo. Localize o campo IP do controlador de computação BMC e navegue até esse IP. 2. Tente restaurar as comunicações BMC colocando o nó no modo de manutenção e, em seguida, desligando e voltando a ligar o aparelho. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG6000 dispositivos de armazenamento 3. Se este alerta persistir, contacte a assistência técnica.
Falha no dispositivo de backup do cache do dispositivo	<p>Um dispositivo de backup de cache persistente falhou.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.
Dispositivo de backup de cache de dispositivo capacidade insuficiente	<p>Não há capacidade insuficiente do dispositivo de backup em cache.</p> <p>Entre em Contato com o suporte técnico.</p>
Dispositivo de backup protegido contra gravação em cache do dispositivo	<p>Um dispositivo de backup em cache está protegido contra gravação.</p> <p>Entre em Contato com o suporte técnico.</p>
Incompatibilidade do tamanho da memória cache do dispositivo	<p>Os dois controladores no dispositivo têm tamanhos de cache diferentes.</p> <p>Entre em Contato com o suporte técnico.</p>

Nome do alerta	Descrição e ações recomendadas
<p>Temperatura do chassi do controlador de computação do dispositivo muito alta</p>	<p>A temperatura do controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.</p> <ol style="list-style-type: none"> 1. Verifique os componentes do hardware quanto a condições de sobreaquecimento e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
<p>Temperatura da CPU do controlador de computação do dispositivo muito alta</p>	<p>A temperatura da CPU no controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.</p> <ol style="list-style-type: none"> 1. Verifique os componentes do hardware quanto a condições de sobreaquecimento e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento

Nome do alerta	Descrição e ações recomendadas
O controlador de computação do dispositivo precisa de atenção	<p>Uma falha de hardware foi detetada no controlador de computação de um dispositivo StorageGRID.</p> <ol style="list-style-type: none"> 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento
A fonte de Alimentação A do controlador de computação do dispositivo tem um problema	<p>A fonte de Alimentação A no controlador de computação tem um problema.este alerta pode indicar que a fonte de alimentação falhou ou que tem um problema de fornecimento de energia.</p> <ol style="list-style-type: none"> 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento

Nome do alerta	Descrição e ações recomendadas
<p>A fonte de alimentação B do controlador de computação do dispositivo tem um problema</p>	<p>A fonte de alimentação B no controlador de computação tem um problema.</p> <p>Este alerta pode indicar que a fonte de alimentação falhou ou que tem um problema de fornecimento de energia.</p> <ol style="list-style-type: none"> 1. Verifique se há erros nos componentes de hardware e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento
<p>O serviço de monitor de hardware de computação do dispositivo parou</p>	<p>O serviço que monitora o status do hardware de storage parou de relatar dados.</p> <ol style="list-style-type: none"> 1. Verifique o estado do serviço de estado do sistema eos na base-os. 2. Se o serviço estiver parado ou em estado de erro, reinicie o serviço. 3. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Detectada avaria no canal de fibra do dispositivo	<p>Foi detetado um problema de link Fibre Channel entre o controlador de storage do dispositivo e o controlador de computação.</p> <p>Esse alerta pode indicar que há um problema com a conexão Fibre Channel entre os controladores de storage e computação no dispositivo.</p> <ol style="list-style-type: none"> 1. Verifique se há erros nos componentes de hardware (NÓS <i>Appliance node hardware</i>). Se o estatuto de qualquer um dos componentes não for "nominal", tomar as seguintes medidas: <ol style="list-style-type: none"> a. Verifique se os cabos Fibre Channel entre os controladores estão completamente conetados. b. Certifique-se de que os cabos Fibre Channel não apresentam dobras excessivas. c. Confirme se os módulos SFP estão devidamente encaixados. <p>Nota: se este problema persistir, o sistema StorageGRID poderá tornar a ligação problemática offline automaticamente.</p> 2. Se necessário, substitua os componentes. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento
Falha na porta HBA Fibre Channel do dispositivo	<p>Uma porta HBA Fibre Channel está falhando ou falhou.</p> <p>Entre em Contato com o suporte técnico.</p>
O cache flash do dispositivo não é ideal	<p>As unidades usadas para o cache SSD não são ideais.</p> <ol style="list-style-type: none"> 1. Substitua as unidades de cache SSD. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Recipiente da bateria/interligação do aparelho removido	<p>O depósito da bateria/interligação está em falta.</p> <ol style="list-style-type: none"> 1. Substitua a bateria. As etapas para remover e substituir uma bateria estão incluídas no procedimento de substituição de um controlador de armazenamento. Consulte as instruções para o seu aparelho de armazenamento. <ul style="list-style-type: none"> ◦ SG5600 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG6000 dispositivos de armazenamento 2. Se este alerta persistir, contacte a assistência técnica.
Porta LACP do aparelho em falta	<p>Uma porta em um dispositivo StorageGRID não está participando da ligação LACP.</p> <ol style="list-style-type: none"> 1. Verifique a configuração do interruptor. Certifique-se de que a interface está configurada no grupo de agregação de links correto. 2. Se este alerta persistir, contacte a assistência técnica.
A fonte de alimentação geral do aparelho está degradada	<p>A alimentação de um aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.</p> <ol style="list-style-type: none"> 1. Verifique o estado das fontes de alimentação A e B para determinar qual fonte de alimentação está a funcionar de forma anormal e siga as ações recomendadas: <ul style="list-style-type: none"> ◦ Se você tiver um SG100, SG1000 ou SG6000, use o BMC. ◦ Se você tiver um SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento ◦ Aparelhos de serviços SG100 e SG1000
Falha do controlador de storage do dispositivo A	<p>O controlador de storage A em um dispositivo StorageGRID falhou.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento

Nome do alerta	Descrição e ações recomendadas
Falha no controlador B de storage do dispositivo	<p>O controlador de storage B em um dispositivo StorageGRID falhou.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
Falha na unidade do controlador de armazenamento do dispositivo	<p>Uma ou mais unidades em um dispositivo StorageGRID falhou ou não é ideal.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
Problema de hardware do controlador de storage do dispositivo	<p>O software SANtricity está relatando "precisa de atenção" para um componente em um dispositivo StorageGRID.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
Falha na fonte de alimentação do controlador de armazenamento do dispositivo	<p>A fonte de Alimentação A num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento

Nome do alerta	Descrição e ações recomendadas
Falha na fonte de alimentação B do controlador de armazenamento do dispositivo	<p>A fonte de alimentação B num aparelho StorageGRID desviou-se da tensão de funcionamento recomendada.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
O serviço de monitor de hardware de armazenamento do dispositivo parou	<p>O serviço que monitora o status do hardware de storage parou de relatar dados.</p> <ol style="list-style-type: none"> 1. Verifique o estado do serviço de estado do sistema eos na base-os. 2. Se o serviço estiver parado ou em estado de erro, reinicie o serviço. 3. Se este alerta persistir, contacte a assistência técnica.
Prateleiras de storage do dispositivo degradadas	<p>O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento é degradado.</p> <ol style="list-style-type: none"> 1. Use o Gerenciador de sistema do SANtricity para verificar os componentes de hardware e siga as ações recomendadas. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento
Temperatura do aparelho excedida	<p>A temperatura nominal ou máxima para o controlador de armazenamento do aparelho foi excedida.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Investigue possíveis razões para o aumento de temperatura, como uma falha da ventoinha ou do sistema de ar condicionado, ventilação e aquecimento (HVAC). 3. Se este alerta persistir, contacte a assistência técnica.
Sensor de temperatura do aparelho removido	<p>Um sensor de temperatura foi removido. Entre em Contato com o suporte técnico.</p>

Nome do alerta	Descrição e ações recomendadas
<p>Erro de auto-compactador Cassandra</p>	<p>O auto-compactador Cassandra sofreu um erro.</p> <p>O compactador automático Cassandra existe em todos os nós de storage e gerencia o tamanho do banco de dados Cassandra para substituir e excluir cargas de trabalho pesadas. Embora essa condição persista, certas cargas de trabalho sofrerão um consumo inesperadamente alto de metadados.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.
<p>Os logs de auditoria estão sendo adicionados à fila na memória</p>	<p>O nó não pode enviar logs para o servidor syslog local e a fila na memória está sendo preenchida.</p> <ol style="list-style-type: none"> 1. Certifique-se de que o serviço rsyslog está em execução no nó. 2. Se necessário, reinicie o serviço rsyslog no nó usando o comando <code>service rsyslog restart</code>. 3. Se o serviço rsyslog não puder ser reiniciado e você não salvar mensagens de auditoria em nós de administração, entre em Contato com o suporte técnico. Os registros de auditoria serão perdidos se esta condição não for corrigida.
<p>Métricas do compactador automático Cassandra desatualizadas</p>	<p>As métricas que descrevem o compactador automático Cassandra estão desatualizadas.</p> <p>O compactador automático Cassandra existe em todos os nós de storage e gerencia o tamanho do banco de dados Cassandra para substituir e excluir cargas de trabalho pesadas. Embora esse alerta persista, certas cargas de trabalho sofrerão um consumo inesperadamente alto de metadados.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Entre em Contato com o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Erro de comunicação Cassandra	<p>Os nós que executam o serviço Cassandra estão tendo problemas para se comunicar uns com os outros.</p> <p>Esse alerta indica que algo está interferindo nas comunicações nó a nó. Pode haver um problema de rede ou o serviço Cassandra pode estar inativo em um ou mais nós de storage.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando um ou mais nós de storage. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Verifique se há um problema de rede que possa estar afetando um ou mais nós de storage. 3. Selecione SUPPORT > Tools > Grid topology. 4. Para cada nó de armazenamento no seu sistema, selecione SSM Serviços. Certifique-se de que o status do serviço Cassandra é "em execução". 5. Se o Cassandra não estiver em execução, siga as etapas para iniciar ou reiniciar um serviço. 6. Se todas as instâncias do serviço Cassandra estiverem em execução e o alerta não for resolvido, entre em Contato com o suporte técnico.
Cassandra compactions sobrecarregado	<p>O processo de compactação Cassandra está sobrecarregado.</p> <p>Se o processo de compactação estiver sobrecarregado, o desempenho de leitura pode estar degradado e a RAM pode ser usada. O serviço Cassandra também pode ficar sem resposta ou falhar.</p> <ol style="list-style-type: none"> 1. Reinicie o serviço Cassandra seguindo as etapas de reiniciar um serviço. 2. Se este alerta persistir, contacte a assistência técnica.
Métricas de reparo do Cassandra desatualizadas	<p>As métricas que descrevem os trabalhos de reparo do Cassandra estão desatualizadas. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos.</p> <ol style="list-style-type: none"> 1. Reinicie o nó. No Gerenciador de Grade, vá para NÓS, selecione o nó e selecione a guia tarefas. 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
O progresso do reparo do Cassandra lento	<p>O progresso dos reparos do banco de dados Cassandra é lento.</p> <p>Quando os reparos do banco de dados são lentos, as operações de consistência de dados do Cassandra são impedidas. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos.</p> <ol style="list-style-type: none"> 1. Confirme se todos os nós de storage estão online e não há alertas relacionados à rede. 2. Monitore esse alerta por até 2 dias para ver se o problema resolve por conta própria. 3. Se as reparações da base de dados continuarem a prosseguir lentamente, contacte a assistência técnica.
O serviço de reparação Cassandra não está disponível	<p>O serviço de reparação Cassandra não está disponível.</p> <p>O serviço de reparo Cassandra existe em todos os nós de storage e fornece funções de reparo críticas para o banco de dados Cassandra. Se essa condição persistir por mais de 48 horas, as consultas de clientes, como listas de intervalos, podem mostrar dados excluídos.</p> <ol style="list-style-type: none"> 1. Selecione SUPPORT > Tools > Grid topology. 2. Para cada nó de armazenamento no seu sistema, selecione SSM Serviços. Certifique-se de que o status do serviço Cassandra Reaper é "em execução". 3. Se o Cassandra Reaper não estiver em execução, siga as etapas para seguir as etapas iniciar ou reiniciar um serviço para . 4. Se todas as instâncias do serviço Cassandra Reaper estiverem em execução e o alerta não for resolvido, entre em Contato com o suporte técnico.
Corrupção da tabela Cassandra	<p>Cassandra detetou corrupção de tabela.</p> <p>O Cassandra reinicia automaticamente se detetar corrupção de tabela.</p> <p>Entre em Contato com o suporte técnico.</p>
Erro de conectividade do Cloud Storage Pool	<p>A verificação de integridade dos pools de armazenamento em nuvem detetou um ou mais erros novos.</p> <ol style="list-style-type: none"> 1. Vá para a seção Cloud Storage Pools da página Storage Pools. 2. Observe a coluna último erro para determinar qual pool de armazenamento em nuvem tem um erro. 3. Consulte as instruções para gerenciamento de objetos com gerenciamento do ciclo de vida das informações.

Nome do alerta	Descrição e ações recomendadas
A concessão DHCP expirou	<p>A concessão de DHCP numa interface de rede expirou. Se a concessão DHCP expirou, siga as ações recomendadas:</p> <ol style="list-style-type: none"> 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte instruções de recuperação e manutenção.
A concessão DHCP expira em breve	<p>A concessão de DHCP em uma interface de rede está expirando em breve.</p> <p>Para evitar que a concessão DHCP expire, siga as ações recomendadas:</p> <ol style="list-style-type: none"> 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte instruções de recuperação e manutenção.
Servidor DHCP indisponível	<p>O servidor DHCP não está disponível.</p> <p>O nó StorageGRID não consegue contactar o servidor DHCP. A concessão DHCP para o endereço IP do nó não pode ser validada.</p> <ol style="list-style-type: none"> 1. Certifique-se de que existe conetividade entre este nó e o servidor DHCP na interface afetada. 2. Certifique-se de que existem endereços IP disponíveis para atribuir na sub-rede afetada no servidor DHCP. 3. Certifique-se de que existe uma reserva permanente para o endereço IP configurado no servidor DHCP. Ou use a ferramenta StorageGRID Change IP para atribuir um endereço IP estático fora do pool de endereços DHCP. Consulte instruções de recuperação e manutenção.

Nome do alerta	Descrição e ações recomendadas
A e/S do disco é muito lenta	<p>E/S de disco muito lento pode estar impactando o desempenho do StorageGRID.</p> <ol style="list-style-type: none"> 1. Se o problema estiver relacionado a um nó de dispositivo de armazenamento, use o Gerenciador de sistema SANtricity para verificar se há unidades com defeito, unidades com falhas previstas ou reparos em andamento. Verifique também o status dos links Fibre Channel ou SAS entre a computação do dispositivo e os controladores de storage para ver se há algum link inativo ou mostrando taxas de erro excessivas. 2. Examine o sistema de armazenamento que hospeda os volumes deste nó para determinar e corrigir a causa raiz da e/S lenta 3. Se este alerta persistir, contacte a assistência técnica. <p>Nota: os nós afetados podem desativar os serviços e reiniciar-se para evitar afetar o desempenho geral da grade. Quando a condição subjacente for limpa e esses nós detetarem o desempenho normal de e/S, eles retornarão ao serviço completo automaticamente.</p>
Falha no rebalanceamento EC	<p>O trabalho para rebalancear os dados codificados por apagamento entre nós de storage falhou ou foi pausado pelo usuário.</p> <ol style="list-style-type: none"> 1. Garantir que todos os nós de storage no local que estão sendo rebalanceados estejam on-line e disponíveis. 2. Certifique-se de que não há falhas de volume no local que está sendo rebalanceado. Se houver, encerre o trabalho EC rebalanceamento para que você possa executar um trabalho de reparo. <pre data-bbox="641 1207 1307 1239">'rebalance-data terminate --job-id <ID>'</pre> <ol style="list-style-type: none"> 3. Certifique-se de que não há falhas de serviço no local sendo rebalanceado. Se um serviço não estiver em execução, siga as etapas para iniciar ou reiniciar um serviço nas instruções de recuperação e manutenção. 4. Depois de resolver quaisquer problemas, reinicie a tarefa executando o seguinte comando no nó de administração principal: <pre data-bbox="641 1533 1242 1564">'rebalance-data start --job-id <ID>'</pre> <ol style="list-style-type: none"> 5. Se não conseguir resolver o problema, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Falha na reparação EC	<p>Um trabalho de reparo para dados codificados de apagamento falhou ou foi interrompido.</p> <ol style="list-style-type: none"> 1. Certifique-se de que existem nós ou volumes de storage disponíveis suficientes para substituir o nó ou o volume de storage com falha. 2. Certifique-se de que haja nós de storage disponíveis suficientes para satisfazer a política de ILM ativa. 3. Certifique-se de que não existem problemas de conectividade de rede. 4. Depois de resolver quaisquer problemas, reinicie a tarefa executando o seguinte comando no nó de administração principal: <pre data-bbox="641 619 1393 682">'repair-data start-ec-node-repair --repair-id <ID>'</pre> 5. Se não conseguir resolver o problema, contacte o suporte técnico.
A reparação CE parou	<p>Um trabalho de reparo para dados codificados de apagamento parou.</p> <ol style="list-style-type: none"> 1. Certifique-se de que existem nós ou volumes de storage disponíveis suficientes para substituir o nó ou o volume de storage com falha. 2. Certifique-se de que não existem problemas de conectividade de rede. 3. Depois de resolver quaisquer problemas, verifique se o alerta está resolvido. Para ver um relatório mais detalhado sobre o progresso da reparação, execute o seguinte comando no nó de administração principal: <pre data-bbox="641 1207 1409 1270">'repair-data show-ec-repair-status --repair-id <ID>'</pre> 4. Se não conseguir resolver o problema, contacte o suporte técnico.


Nome do alerta	Descrição e ações recomendadas
Falha na notificação por e-mail	<p>Não foi possível enviar a notificação por e-mail para um alerta.</p> <p>Este alerta é acionado quando uma notificação por e-mail de alerta falhar ou um e-mail de teste (enviado da página ALERTAS Configuração de e-mail) não pode ser entregue.</p> <ol style="list-style-type: none"> 1. Inicie sessão no Grid Manager a partir do Admin Node listado na coluna Site/nó do alerta. 2. Vá para a página ALERTAS Configuração de e-mail, verifique as configurações e altere-as, se necessário. 3. Clique em Enviar e-mail de teste e verifique a caixa de entrada de um destinatário de teste para o e-mail. Uma nova instância desse alerta pode ser acionada se o e-mail de teste não puder ser enviado. 4. Se o e-mail de teste não puder ser enviado, confirme se o servidor de e-mail está online. 5. Se o servidor estiver funcionando, selecione support Tools Logs e colete o log para o Admin Node. Especifique um período de tempo que seja de 15 minutos antes e depois da hora do alerta. 6. Extraia o arquivo baixado e revise o conteúdo do <code>prometheus.log</code> (<code>_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log</code>). 7. Se não conseguir resolver o problema, contacte o suporte técnico.
Expiração dos certificados de cliente configurados na página certificados	<p>Um ou mais certificados de cliente configurados na página certificados estão prestes a expirar.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione CONFIGURATION > Security > Certificates e, em seguida, selecione a guia Client. 2. Selecione um certificado que expirará em breve. 3. Selecione Anexar novo certificado ao carregue ou gere um novo certificado. 4. Repita estas etapas para cada certificado que expirará em breve.

Nome do alerta	Descrição e ações recomendadas
Expiração do certificado de ponto final do balanceador de carga	<p>Um ou mais certificados de endpoint do balanceador de carga estão prestes a expirar.</p> <ol style="list-style-type: none"> 1. Selecione CONFIGURATION > Network > Load balancer endpoints. 2. Selecione um endpoint que tenha um certificado que expirará em breve. 3. Selecione Editar endpoint para carregar ou gerar um novo certificado. 4. Repita essas etapas para cada ponto final que tenha um certificado expirado ou que expirará em breve. <p>Para obter mais informações sobre como gerenciar os pontos de extremidade do balanceador de carga, consulte o Instruções para administrar o StorageGRID.</p>
Expiração do certificado de servidor para interface de gerenciamento	<p>O certificado do servidor usado para a interface de gerenciamento está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Selecione CONFIGURATION > Security > Certificates. 2. Na guia Global, selecione certificado de interface de gerenciamento. 3. Carregue um novo certificado de interface de gerenciamento.
Expiração do certificado de servidor global para S3 e Swift API	<p>O certificado do servidor usado para acessar endpoints da 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.
Expiração do certificado CA do syslog externo	<p>O certificado de autoridade de certificação (CA) usado para assinar o certificado de servidor syslog externo está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Atualize o certificado CA no servidor syslog externo. 2. Obtenha uma cópia do certificado de CA atualizado. 3. No Gerenciador de Grade, vá para CONFIGURATION Monitoring Audit and syslog Server. 4. Selecione Editar servidor syslog externo. 5. Selecione Procurar para carregar o novo certificado. 6. Conclua o assistente de configuração para salvar o novo certificado e a chave.

Nome do alerta	Descrição e ações recomendadas
Expiração do certificado do cliente syslog externo	<p>O certificado de cliente para um servidor syslog externo está prestes a expirar.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, vá para CONFIGURATION Monitoring Audit and syslog Server. 2. Selecione Editar servidor syslog externo. 3. Selecione Procurar para carregar o novo certificado. 4. Selecione Procurar para carregar a nova chave privada. 5. Conclua o assistente de configuração para salvar o novo certificado e a chave.
Expiração do certificado do servidor syslog externo	<p>O certificado de servidor apresentado pelo servidor syslog externo está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Atualize o certificado do servidor no servidor syslog externo. 2. Se você usou anteriormente a API do Grid Manager para fornecer um certificado de servidor para validação de certificado, faça o upload do certificado de servidor atualizado usando a API.
Erro de encaminhamento do servidor syslog externo	<p>O nó não pode encaminhar logs para o servidor syslog externo.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, vá para CONFIGURATION Monitoring Audit and syslog Server. 2. Selecione Editar servidor syslog externo. 3. Avance pelo assistente de configuração até selecionar Enviar mensagens de teste. 4. Selecione Enviar mensagens de teste para determinar por que os logs não podem ser encaminhados para o servidor syslog externo. 5. Resolva quaisquer problemas relatados.
Incompatibilidade da MTU da rede da grelha	<p>A configuração MTU (Maximum Transmission Unit) para a interface Grid Network (eth0) difere significativamente entre nós na grade.</p> <p>As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 são configuradas para quadros jumbo. Uma incompatibilidade de tamanho da MTU superior a 1000 pode causar problemas de desempenho da rede.</p> <p>Consulte as instruções para o alerta de incompatibilidade da MTU da rede de Grade Solucionar problemas de rede, hardware e plataformaem.</p>

Nome do alerta	Descrição e ações recomendadas
Alto uso de heap Java	<p>Uma alta porcentagem de espaço de heap Java está sendo usada.</p> <p>Se o heap Java ficar cheio, os serviços de metadados podem ficar indisponíveis e as solicitações do cliente podem falhar.</p> <ol style="list-style-type: none"> 1. Reveja a atividade do ILM no Dashboard. Esse alerta pode ser resolvido por conta própria quando a carga de trabalho do ILM diminui. 2. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 3. Se este alerta persistir, contacte a assistência técnica.
Alta latência para consultas de metadados	<p>O tempo médio para consultas de metadados do Cassandra é muito longo.</p> <p>Um aumento na latência da consulta pode ser causado por uma alteração de hardware, como a substituição de um disco, uma mudança de carga de trabalho, como um aumento súbito de ingerências ou uma mudança de rede, como um problema de comunicação entre nós e sites.</p> <ol style="list-style-type: none"> 1. Determine se houve alguma alteração de hardware, carga de trabalho ou rede no momento em que a latência da consulta aumentou. 2. Se não conseguir resolver o problema, contacte o suporte técnico.
Falha na sincronização da federação de identidade	<p>Não é possível sincronizar grupos federados e usuários da origem da identidade.</p> <ol style="list-style-type: none"> 1. Confirme se o servidor LDAP configurado está online e disponível. 2. Revise as configurações na página Federação de identidade. Confirme se todos os valores são atuais. Consulte Use a federação de identidade as instruções para administrar o StorageGRID. 3. Clique em Test Connection para validar as configurações do servidor LDAP. 4. Se não conseguir resolver o problema, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Falha na sincronização da federação de identidade para um locatário	<p>Não é possível sincronizar grupos federados e usuários da origem de identidade configurada por um locatário.</p> <ol style="list-style-type: none"> 1. Inicie sessão no Gestor do Locatário. 2. Confirme se o servidor LDAP configurado pelo locatário está online e disponível. 3. Revise as configurações na página Federação de identidade. Confirme se todos os valores são atuais. Consulte Use a federação de identidade as instruções para usar uma conta de locatário. 4. Clique em Test Connection para validar as configurações do servidor LDAP. 5. Se não conseguir resolver o problema, contacte o suporte técnico.
Colocação de ILM inalcançável	<p>Uma instrução de colocação em uma regra ILM não pode ser alcançada para determinados objetos.</p> <p>Este alerta indica que um nó exigido por uma instrução de colocação não está disponível ou que uma regra ILM está mal configurada. Por exemplo, uma regra pode especificar mais cópias replicadas do que há nós de storage.</p> <ol style="list-style-type: none"> 1. Certifique-se de que todos os nós estejam online. 2. Se todos os nós estiverem on-line, revise as instruções de posicionamento em todas as regras ILM usadas na política ILM ativa. Confirme se existem instruções válidas para todos os objetos. Consulte instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações. 3. Conforme necessário, atualize as configurações das regras e ative uma nova política. <p>Nota: pode demorar até 1 dia para que o alerta seja apagado.</p> <ol style="list-style-type: none"> 4. Se o problema persistir, entre em Contato com o suporte técnico. <p>Nota: este alerta pode aparecer durante uma atualização e pode persistir por 1 dia após a atualização ser concluída com sucesso. Quando esse alerta é acionado por uma atualização, ele será apagado por conta própria.</p>

Nome do alerta	Descrição e ações recomendadas
<p>Período de digitalização ILM demasiado longo</p>	<p>O tempo necessário para digitalizar, avaliar objetos e aplicar ILM é muito longo.</p> <p>Se o tempo estimado para concluir uma varredura ILM completa de todos os objetos for muito longo (consulte período de digitalização - estimado no Painel de instrumentos), a política ILM ativa pode não ser aplicada a objetos recém-ingeridos. As alterações à política ILM podem não ser aplicadas a objetos existentes.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Confirme se todos os nós de storage estão online. 3. Reduza temporariamente a quantidade de tráfego do cliente. Por exemplo, no Gerenciador de Grade, selecione CONFIGURAÇÃO rede classificação de tráfego e crie uma política que limite a largura de banda ou o número de solicitações. 4. Se a e/S de disco ou a CPU estiverem sobrecarregadas, tente reduzir a carga ou aumentar o recurso. 5. Se necessário, atualize as regras do ILM para usar o posicionamento síncrono (padrão para regras criadas após o StorageGRID 11,3). 6. Se este alerta persistir, contacte a assistência técnica. <p>Administrar o StorageGRID</p>
<p>Taxa de digitalização ILM baixa</p>	<p>A taxa de digitalização ILM é definida para menos de 100 objetos/segundo.</p> <p>Este alerta indica que alguém alterou a taxa de digitalização ILM para o seu sistema para menos de 100 objetos/segundo (predefinição: 400 objetos/segundo). A política ILM ativa pode não ser aplicada a objetos recém-ingeridos. As alterações subsequentes à política ILM não serão aplicadas a objetos existentes.</p> <ol style="list-style-type: none"> 1. Determine se foi efetuada uma alteração temporária à taxa de digitalização ILM como parte de uma investigação de suporte em curso. 2. Entre em Contato com o suporte técnico. <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Nunca altere a taxa de digitalização ILM sem contactar o suporte técnico.</p> </div>

Nome do alerta	Descrição e ações recomendadas
Expiração do certificado CA de KMS	<p>O certificado de autoridade de certificação (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Usando o software KMS, atualize o certificado da CA para o servidor de gerenciamento de chaves. 2. No Gerenciador de Grade, selecione CONFIGURATION Security Key Management Server. 3. Selecione o KMS que tem um aviso de status de certificado. 4. Selecione Editar. 5. Selecione Next para ir para a Etapa 2 (carregar certificado do servidor). 6. Selecione Procurar para carregar o novo certificado. 7. Selecione Guardar. <p>Administrar o StorageGRID</p>
Expiração do certificado do cliente KMS	<p>O certificado de cliente para um servidor de gerenciamento de chaves está prestes a expirar.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione CONFIGURATION Security Key Management Server. 2. Selecione o KMS que tem um aviso de status de certificado. 3. Selecione Editar. 4. Selecione Next para ir para a Etapa 3 (carregar certificados de cliente). 5. Selecione Procurar para carregar o novo certificado. 6. Selecione Procurar para carregar a nova chave privada. 7. Selecione Guardar. <p>Administrar o StorageGRID</p>
Falha ao carregar a configuração DE KMS	<p>A configuração para o servidor de gerenciamento de chaves existe, mas não foi possível carregar.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Se este alerta persistir, contacte a assistência técnica.

Nome do alerta	Descrição e ações recomendadas
Erro de conectividade DE KMS	<p>Um nó de dispositivo não pôde se conectar ao servidor de gerenciamento de chaves para seu site.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione CONFIGURATION Security Key Management Server. 2. Confirme se as entradas da porta e do nome do host estão corretas. 3. Confirme se o certificado do servidor, o certificado do cliente e a chave privada do certificado do cliente estão corretos e não expiraram. 4. Certifique-se de que as definições da firewall permitem que o nó do dispositivo comunique com o KMS especificado. 5. Corrija quaisquer problemas de rede ou DNS. 6. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.
Nome da chave de encriptação KMS não encontrado	<p>O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido.</p> <ol style="list-style-type: none"> 1. Confirme se o KMS atribuído ao site está usando o nome correto para a chave de criptografia e quaisquer versões anteriores. 2. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.
Falha na rotação da chave de CRIPTOGRAFIA KMS	<p>Todos os volumes de appliance foram descriptografados, mas um ou mais volumes não puderam girar para a chave mais recente. Contate o suporte técnico.</p>
KMS não está configurado	<p>Não existe nenhum servidor de gerenciamento de chaves para este site.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione CONFIGURATION Security Key Management Server. 2. Adicione um KMS para este site ou adicione um KMS padrão. <p>Administrar o StorageGRID</p>
A chave KMS falhou ao descriptar um volume de aparelho	<p>Um ou mais volumes em um dispositivo com criptografia de nó ativada não puderam ser descriptografados com a chave KMS atual.</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Certifique-se de que o servidor de gerenciamento de chaves (KMS) tenha a chave de criptografia configurada e quaisquer versões anteriores de chaves. 3. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Expiração do certificado do servidor DE KMS	<p>O certificado do servidor usado pelo KMS (Key Management Server) está prestes a expirar.</p> <ol style="list-style-type: none"> 1. Usando o software KMS, atualize o certificado do servidor para o servidor de gerenciamento de chaves. 2. Se precisar de assistência ou este alerta persistir, contacte o suporte técnico. <p>Administrar o StorageGRID</p>
Fila de auditoria grande	<p>A fila de discos para mensagens de auditoria está cheia.</p> <ol style="list-style-type: none"> 1. Verifique a carga no sistema - se houve um número significativo de transações, o alerta deve resolver-se ao longo do tempo, e você pode ignorar o alerta. 2. Se o alerta persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. 3. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado (CONFIGURAÇÃO Monitoramento servidor de auditoria e syslog). <p>Rever registos de auditoria</p>
Detetada atividade do balanceador de carga CLB legada	<p>Alguns clientes podem estar se conetando ao serviço de balanceador de carga CLB obsoleto usando o certificado padrão S3 e Swift API.</p> <ol style="list-style-type: none"> 1. Para simplificar futuras atualizações, instale um certificado API S3 e Swift personalizado na guia Global da página certificados. Em seguida, certifique-se de que todos os clientes S3 ou Swift que se conetam ao CLB legado tenham o novo certificado. 2. Crie um ou mais pontos de extremidade do balanceador de carga. Em seguida, direcione todos os clientes S3 e Swift existentes para esses endpoints. Entre em Contato com o suporte técnico se precisar remapear a porta do cliente. <p>Outras atividades podem acionar este alerta, incluindo as verificações de portas. Para determinar se o serviço CLB obsoleto está atualmente em uso, veja a <code>storagegrid_private_clb_http_connection_established_successful</code> métrica Prometheus.</p> <p>Conforme necessário, silencie ou desative essa regra de alerta se o serviço CLB não estiver mais em uso.</p>

Nome do alerta	Descrição e ações recomendadas
Os logs estão sendo adicionados à fila no disco	<p>O nó não pode encaminhar logs para o servidor syslog externo e a fila no disco está sendo preenchida.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, vá para CONFIGURATION Monitoring Audit and syslog Server. 2. Selecione Editar servidor syslog externo. 3. Avance pelo assistente de configuração até selecionar Enviar mensagens de teste. 4. Selecione Enviar mensagens de teste para determinar por que os logs não podem ser encaminhados para o servidor syslog externo. 5. Resolva quaisquer problemas relatados.
Baixa capacidade de disco de log de auditoria	<p>O espaço disponível para logs de auditoria é baixo.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Baixa memória disponível do nó	<p>A quantidade de RAM disponível em um nó é baixa.</p> <p>A baixa RAM disponível pode indicar uma alteração na carga de trabalho ou um vazamento de memória com um ou mais nós.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve por conta própria. 2. Se a memória disponível descer abaixo do limite de alerta principal, contacte o suporte técnico.
Baixo espaço livre para piscina de armazenamento	<p>A quantidade de espaço disponível para armazenar dados de objetos em um pool de armazenamento é baixa.</p> <ol style="list-style-type: none"> 1. Selecione ILM > Storage Pools. 2. Selecione o pool de armazenamento listado no alerta e selecione Exibir detalhes. 3. Determine onde a capacidade de armazenamento adicional é necessária. Você pode adicionar nós de storage a cada local no pool de storage ou adicionar volumes de storage (LUNs) a um ou mais nós de storage existentes. 4. Execute um procedimento de expansão para aumentar a capacidade de armazenamento. <p>Expanda sua grade</p>

Nome do alerta	Descrição e ações recomendadas
Baixa memória do nó instalada	<p>A quantidade de memória instalada em um nó é baixa.</p> <p>Aumente a quantidade de RAM disponível para a máquina virtual ou host Linux. Verifique o valor de limite do alerta principal para determinar o requisito mínimo padrão para um nó StorageGRID. Consulte as instruções de instalação da sua plataforma:</p> <ul style="list-style-type: none"> • Instale o Red Hat Enterprise Linux ou CentOS • Instale Ubuntu ou Debian • Instale o VMware
Baixo armazenamento de metadados	<p>O espaço disponível para armazenar metadados de objetos é baixo.</p> <p>Alerta crítico</p> <ol style="list-style-type: none"> 1. Pare de ingerir objetos. 2. Adicione imediatamente nós de storage em um procedimento de expansão. <p>Alerta principal</p> <p>Adicione imediatamente nós de storage em um procedimento de expansão.</p> <p>Menor alerta</p> <ol style="list-style-type: none"> 1. Monitore a taxa na qual o espaço de metadados de objetos está sendo usado. Selecione NÓS Storage Node Storage e veja o gráfico Storage Used - Object Metadata. 2. Adicione nós de storage em um procedimento de expansão o mais rápido possível. <p>Depois que novos nós de storage são adicionados, o sistema reequilibra automaticamente os metadados de objetos em todos os nós de storage e o alarme é apagado.</p> <p>Consulte as instruções para o alerta de armazenamento de metadados baixos no Solucionar problemas de metadados.</p>
Baixa capacidade de disco de métricas	<p>O espaço disponível para o banco de dados de métricas é baixo.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.

Nome do alerta	Descrição e ações recomendadas
Baixo armazenamento de dados de objetos	<p>O espaço disponível para armazenar dados de objetos é baixo.</p> <p>Execute um procedimento de expansão. Você pode adicionar volumes de storage (LUNs) aos nós de storage existentes ou adicionar novos nós de storage.</p> <p>Solucionar problemas do alerta de armazenamento de dados de objetos baixos</p> <p>Expanda sua grade</p>
Baixa sobreposição de marca d'água somente leitura	<p>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.</p> <p>Para saber como resolver este alerta, vá para Solucionar problemas de alertas de substituição de marca d'água somente leitura baixa.</p>
Baixa capacidade de disco raiz	<p>O espaço disponível para o disco raiz é baixo.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Baixa capacidade de dados do sistema	<p>O espaço disponível para os dados do sistema StorageGRID no <code>/var/local</code> sistema de arquivos é baixo.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Espaço livre do diretório de baixa tmp	<p>O espaço disponível no diretório <code>/tmp</code> é baixo.</p> <ol style="list-style-type: none"> 1. Monitore esse alerta para ver se o problema resolve sozinho e o espaço em disco se torna disponível novamente. 2. Contacte o suporte técnico se o espaço disponível continuar a diminuir.
Erro de conectividade de rede do nó	<p>Ocorreram erros durante a transferência de dados entre nós.</p> <p>Os erros de conectividade de rede podem ser apagados sem intervenção manual. Entre em Contato com o suporte técnico se os erros não forem claros.</p> <p>Consulte as instruções para o alarme Network Receive Error (NRER) em Solucionar problemas de rede, hardware e plataforma.</p>

Nome do alerta	Descrição e ações recomendadas
<p>Erro de quadro de recepção de rede do nó</p>	<p>Uma alta porcentagem dos quadros de rede recebidos por um nó teve erros.</p> <p>Esse alerta pode indicar um problema de hardware, como um cabo com defeito ou um transceptor com falha em qualquer uma das extremidades da conexão Ethernet.</p> <ol style="list-style-type: none"> 1. Se você estiver usando um dispositivo, tente substituir cada transceptor SFP ou SFP28 e cabo, um de cada vez, para ver se o alerta é apagado. 2. Se este alerta persistir, contacte a assistência técnica.
<p>Nó não sincronizado com o servidor NTP</p>	<p>A hora do nó não está sincronizada com o servidor NTP (Network Time Protocol).</p> <ol style="list-style-type: none"> 1. Verifique se você especificou pelo menos quatro servidores NTP externos, cada um fornecendo uma referência estrato 3 ou melhor. 2. Verifique se todos os servidores NTP estão operando normalmente. 3. Verifique as conexões com os servidores NTP. Certifique-se de que eles não estão bloqueados por um firewall.
<p>Nó não bloqueado com servidor NTP</p>	<p>O nó não está bloqueado para um servidor NTP (Network Time Protocol).</p> <ol style="list-style-type: none"> 1. Verifique se você especificou pelo menos quatro servidores NTP externos, cada um fornecendo uma referência estrato 3 ou melhor. 2. Verifique se todos os servidores NTP estão operando normalmente. 3. Verifique as conexões com os servidores NTP. Certifique-se de que eles não estão bloqueados por um firewall.
<p>Rede do nó que não é do dispositivo inativa</p>	<p>Um ou mais dispositivos de rede estão inativos ou desconetados. Este alerta indica que uma interface de rede (eth) para um nó instalado em uma máquina virtual ou host Linux não está acessível.</p> <p>Entre em Contato com o suporte técnico.</p>

Nome do alerta	Descrição e ações recomendadas
Falha na verificação de existência do objeto	<p>O trabalho de verificação de existência de objeto falhou.</p> <ol style="list-style-type: none"> 1. Selecione MAINTENANCE Object existence check. 2. Anote a mensagem de erro. Execute as ações corretivas apropriadas: <ul style="list-style-type: none"> Falha ao iniciar, conexão perdida, erro desconhecido a. Certifique-se de que os nós de storage e os volumes incluídos no trabalho estejam on-line e disponíveis. b. Certifique-se de que não haja falhas de serviço ou volume nos nós de storage. Se um serviço não estiver em execução, inicie ou reinicie o serviço. Consulte instruções de recuperação e manutenção. c. Certifique-se de que o controle de consistência selecionado pode ser satisfeito. d. Depois de resolver quaisquer problemas, selecione Repetir. O trabalho será retomado a partir do último estado válido. Erro crítico de armazenamento no volume e. Recupere o volume com falha. Consulte instruções de recuperação e manutenção. f. Selecione Repetir. g. Após a conclusão do trabalho, crie outro trabalho para os volumes restantes no nó para verificar se há erros adicionais. 3. Se você não conseguir resolver os problemas, entre em Contato com o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Verificação de existência de objeto parada	<p>O trabalho de verificação de existência de objeto parou.</p> <p>O trabalho de verificação de existência de objeto não pode continuar. Um ou mais nós de storage ou volumes incluídos na tarefa estão offline ou não respondem, ou o controle de consistência selecionado não pode mais ser satisfeito porque muitos nós estão inativos ou indisponíveis.</p> <ol style="list-style-type: none"> 1. Certifique-se de que todos os nós e volumes de storage verificados estejam online e disponíveis (selecione NÓS). 2. Certifique-se de que nós de storage suficientes estejam online e disponíveis para permitir que o nó coordenador atual leia metadados de objetos usando o controle de consistência selecionado. Se necessário, inicie ou reinicie um serviço. Consulte instruções de recuperação e manutenção. <p>Quando resolver os passos 1 e 2, o trabalho inicia-se automaticamente de onde parou.</p> <ol style="list-style-type: none"> 3. Se o controle de consistência selecionado não puder ser satisfeito, cancele o trabalho e inicie outro trabalho utilizando um controle de consistência inferior. 4. Se você não conseguir resolver os problemas, entre em Contato com o suporte técnico.
Objetos perdidos	<p>Um ou mais objetos foram perdidos da grade.</p> <p>Esse alerta pode indicar que os dados foram perdidos permanentemente e não podem ser recuperados.</p> <ol style="list-style-type: none"> 1. Investigue este alerta imediatamente. Talvez seja necessário tomar medidas para evitar mais perda de dados. Você também pode restaurar um objeto perdido se você executar uma ação de prompt. <p style="margin-left: 20px;">Solucionar problemas de dados de objetos perdidos e ausentes</p> 2. Quando o problema subjacente for resolvido, reinicie o contador: <ol style="list-style-type: none"> a. Selecione SUPPORT > Tools > Grid topology. b. Para o nó de armazenamento que levantou o alerta, selecione site grid node LDR Data Store Configuration Main. c. Selecione Redefinir contagem de objetos perdidos e clique em aplicar alterações.

Nome do alerta	Descrição e ações recomendadas
Serviços de plataforma indisponíveis	<p>Poucos nós de storage com o serviço RSM estão em execução ou disponíveis em um local.</p> <p>Certifique-se de que a maioria dos nós de storage que têm o serviço RSM no local afetado esteja em execução e em um estado não-erro.</p> <p>Consulte ""solução de problemas de serviços de plataforma"" no Instruções para administrar o StorageGRID.</p>
S3 COLOQUE o tamanho do objeto muito grande	<p>Um cliente S3 está tentando executar uma operação PUT Object que excede os limites de tamanho S3.</p> <ol style="list-style-type: none"> 1. Use o ID do locatário mostrado nos detalhes do alerta para identificar a conta do locatário. 2. Vá para suporte Ferramentas Logs e colete os Logs de aplicativos para o nó de armazenamento mostrado nos detalhes do alerta. Especifique um período de tempo que seja de 15 minutos antes e depois da hora do alerta. 3. Extraia o arquivo baixado e navegue até o local do <code>bycast.log (/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log)</code>. 4. Procure o conteúdo de <code>bycast.log "method=PUT"</code> e identifique o endereço IP do cliente S3 olhando para o <code>clientIP</code> campo. 5. Informe a todos os usuários do cliente que o tamanho máximo do objeto PUT é de 5 GiB. 6. Use uploads multipart para objetos maiores que 5 GiB.
Link do utilitário de serviços para baixo na porta de rede Admin 1	<p>A porta Admin Network 1 do aparelho está inativa ou desconetada.</p> <ol style="list-style-type: none"> 1. Verifique o cabo e a conexão física à porta Admin Network 1. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ Desativar regras de alerta

Nome do alerta	Descrição e ações recomendadas
<p>Link do utilitário de serviços para baixo na rede de administração (ou rede de cliente)</p>	<p>A interface do dispositivo para a rede de administração (eth1) ou a rede de cliente (eth2) está inativa ou desligada.</p> <ol style="list-style-type: none"> 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ Desativar regras de alerta
<p>O utilitário de serviços está conetado na porta de rede 1, 2, 3 ou 4</p>	<p>A porta de rede 1, 2, 3 ou 4 do aparelho está inativa ou desligada.</p> <ol style="list-style-type: none"> 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ Aparelhos de serviços SG100 e SG1000 ◦ Desativar regras de alerta

Nome do alerta	Descrição e ações recomendadas
<p>Conectividade de storage do dispositivo de serviços degradada</p>	<p>Um dos dois SSDs em um dispositivo de serviços falhou ou está fora de sincronização com o outro.</p> <p>A funcionalidade do dispositivo não é afetada, mas você deve resolver o problema imediatamente. Se ambas as unidades falharem, o aparelho deixará de funcionar.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione NÓS Services Appliance e, em seguida, selecione a guia hardware. 2. Reveja a mensagem no campo Storage RAID Mode (modo RAID de armazenamento*). 3. Se a mensagem mostrar o andamento de uma operação de resincronização, aguarde a conclusão da operação e confirme se o alerta foi resolvido. Uma mensagem de resincronização significa que o SSD foi substituído recentemente ou que está sendo resincronizado por outro motivo. 4. Se a mensagem indicar que um dos SSDs falhou, substitua a unidade com falha o mais rápido possível. <p>Para obter instruções sobre como substituir uma unidade em um dispositivo de serviços, consulte o guia de instalação e manutenção dos aparelhos SG100 e SG1000.</p> <p>Aparelhos de serviços SG100 e SG1000</p>
<p>Link do dispositivo de armazenamento na porta Admin Network 1</p>	<p>A porta Admin Network 1 do aparelho está inativa ou desconetada.</p> <ol style="list-style-type: none"> 1. Verifique o cabo e a conexão física à porta Admin Network 1. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento ◦ Desativar regras de alerta

Nome do alerta	Descrição e ações recomendadas
Link do dispositivo de armazenamento na rede Admin (ou rede do cliente)	<p>A interface do dispositivo para a rede de administração (eth1) ou a rede de cliente (eth2) está inativa ou desligada.</p> <ol style="list-style-type: none"> 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento ◦ Desativar regras de alerta
Ligação do dispositivo de armazenamento na porta de rede 1, 2, 3 ou 4	<p>A porta de rede 1, 2, 3 ou 4 do aparelho está inativa ou desligada.</p> <ol style="list-style-type: none"> 1. Verifique os cabos, SFPs e conexões físicas à rede StorageGRID. 2. Solucione quaisquer problemas de conexão. Consulte as instruções de instalação e manutenção do hardware do seu aparelho. 3. Se esta porta estiver desconetada de propósito, desative esta regra. No Gerenciador de Grade, selecione ALERTAS regras, selecione a regra e clique em Editar regra. Em seguida, desmarque a caixa de seleção Enabled. <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento ◦ Desativar regras de alerta

Nome do alerta	Descrição e ações recomendadas
Conectividade de storage do dispositivo de storage degradada	<p>Há um problema com uma ou mais conexões entre o controlador de computação e o controlador de storage.</p> <ol style="list-style-type: none"> 1. Vá ao aparelho para verificar as luzes indicadoras da porta. 2. Se as luzes de uma porta estiverem apagadas, confirme se o cabo está conetado corretamente. Conforme necessário, substitua o cabo. 3. Aguarde até cinco minutos. <p>Nota: se for necessário substituir um segundo cabo, não o desligue durante pelo menos 5 minutos. Caso contrário, o volume raiz pode se tornar somente leitura, o que requer uma reinicialização de hardware.</p> <ol style="list-style-type: none"> 4. No Gerenciador de Grade, selecione NÓS. Em seguida, selecione a guia hardware do nó que teve o problema. Verifique se a condição de alerta foi resolvida.
Dispositivo de armazenamento inacessível	<p>Não é possível aceder a um dispositivo de armazenamento.</p> <p>Este alerta indica que um volume não pode ser montado ou acessado devido a um problema com um dispositivo de armazenamento subjacente.</p> <ol style="list-style-type: none"> 1. Verifique o status de todos os dispositivos de armazenamento usados para o nó: <ul style="list-style-type: none"> ◦ Se o nó estiver instalado em uma máquina virtual ou em um host Linux, siga as instruções para que seu sistema operacional execute diagnósticos de hardware ou execute uma verificação do sistema de arquivos. <ul style="list-style-type: none"> ▪ Instale o Red Hat Enterprise Linux ou CentOS ▪ Instale Ubuntu ou Debian ▪ Instale o VMware ◦ Se o nó estiver instalado em um dispositivo SG100, SG1000 ou SG6000, use o BMC. ◦ Se o nó estiver instalado em um dispositivo SG5600 ou SG5700, use o Gerenciador de sistema do SANtricity. 2. Se necessário, substituir o órgão. Consulte as instruções do seu aparelho: <ul style="list-style-type: none"> ◦ SG6000 dispositivos de armazenamento ◦ SG5700 dispositivos de armazenamento ◦ SG5600 dispositivos de armazenamento

Nome do alerta	Descrição e ações recomendadas
Uso de cota de locatário alto	<p>Uma alta porcentagem de espaço de cota de locatário está sendo usada. Se um inquilino exceder sua cota, novos ingerências são rejeitados.</p> <p>Nota: esta regra de alerta é desativada por padrão porque pode gerar muitas notificações.</p> <ol style="list-style-type: none"> 1. No Gerenciador de Grade, selecione TENANTS. 2. Classifique a tabela por quota de utilização. 3. Selecione um locatário cuja utilização da cota seja próxima de 100%. 4. Faça um ou ambos os procedimentos a seguir: <ul style="list-style-type: none"> ◦ Selecione Editar para aumentar a cota de armazenamento do locatário. ◦ Notificar o locatário de que a utilização da cota é alta.
Não é possível comunicar com o nó	<p>Um ou mais serviços não respondem ou o nó não pode ser alcançado.</p> <p>Este alerta indica que um nó está desconetado por um motivo desconhecido. 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>Monitore esse alerta para ver se o problema resolve por conta própria. Se o problema persistir:</p> <ol style="list-style-type: none"> 1. Determine se há outro alerta afetando esse nó. Esse alerta pode ser resolvido quando você resolver o outro alerta. 2. Confirme se todos os serviços neste nó estão em execução. Se um serviço for interrompido, tente iniciá-lo. Consulte instruções de recuperação e manutenção. 3. Certifique-se de que o host do nó esteja ligado. Se não estiver, inicie o host. <p>Observação: se mais de um host for desligado, consulte instruções de recuperação e manutenção.</p> <ol style="list-style-type: none"> 4. Determine se há um problema de conectividade de rede entre este nó e o nó Admin. 5. Se não conseguir resolver o alerta, contacte o suporte técnico.

Nome do alerta	Descrição e ações recomendadas
Reinicialização inesperada do nó	<p>Um nó reinicializou inesperadamente nas últimas 24 horas.</p> <ol style="list-style-type: none"> 1. Monitorize este alerta. O alerta será apagado após 24 horas. No entanto, se o nó reiniciar inesperadamente novamente, este alerta será acionado novamente. 2. Se você não conseguir resolver o alerta, pode haver uma falha de hardware. Entre em Contato com o suporte técnico.
Objeto corrompido não identificado detetado	<p>Um arquivo foi encontrado no storage de objetos replicado que não pôde ser identificado como um objeto replicado.</p> <ol style="list-style-type: none"> 1. Determine se há algum problema com o storage subjacente em um nó de storage. Por exemplo, execute diagnósticos de hardware ou execute uma verificação do sistema de arquivos. 2. Depois de resolver quaisquer problemas de storage, executar verificação de existência de objeto para determinar se as cópias replicadas, conforme definido pela política de ILM, estão ausentes. 3. Monitorize este alerta. O alerta será apagado após 24 horas, mas será acionado novamente se o problema não tiver sido corrigido. 4. Se não conseguir resolver o alerta, contacte o suporte técnico.

Métricas de Prometheus comumente usadas

O serviço Prometheus nos Admin Nodes coleta métricas de séries temporais dos serviços em todos os nós. Enquanto Prometheus coleta mais de mil métricas, um número relativamente pequeno é necessário para monitorar as operações mais críticas do StorageGRID.

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.

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.

A tabela a seguir lista as métricas mais usadas do Prometheus. Você pode consultar esta lista para entender melhor as condições nas regras de alerta padrão ou para construir as condições para regras de alerta personalizadas.



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.

Métrica Prometheus	Descrição
alertmanager_notifications_failed_total	O número total de notificações de alerta com falha.
node_filesystem_avail_bytes	A quantidade de espaço de 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 de /sys/class/net/iface.
node_network_receive_errs_total	Estatísticas do dispositivo de rede Receive_errs.
node_network_transmit_errs_total	Estatísticas 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

Métrica Prometheus	Descrição
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.

Métrica Prometheus	Descrição
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_miliseconds	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_endpoint_s_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.

Métrica Prometheus	Descrição
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: <ul style="list-style-type: none"> • 10: Offline • 15: Manutenção • 20 - somente leitura • 30 - Online
StorageGRID_storage_status	O status atual dos serviços de storage. Os valores de atributo são: <ul style="list-style-type: none"> • 0: Sem erros • 10: Em transição • 20: Espaço livre insuficiente • 30 volume(s) indisponível(s) • 40 - erro
StorageGRID_storage_utilization_bytes	Uma estimativa do tamanho total dos dados de objetos codificados de apagamento e replicados no nó de storage.

Métrica Prometheus	Descrição
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.

Métrica Prometheus	Descrição
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.

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>
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>

Código	Nome	Serviço	Ação recomendada
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 Alarms 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 logConsulte .</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 multipath aparecer como ""degradado"" (selecione SUPORTE Ferramentas topologia de grade, selecione site grid node SSM Eventos), 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 Resources e verifique se o status do Multipath ""degradado"" mudou 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>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 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 de 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 sobreaquecimento. 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 Dashboard 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>
CAIH	Número disponível ingest Destinations	CLB	Este alarme está obsoleto.
CAQH	Número de destinos disponíveis	CLB	<p>Este alarme é apagado quando os problemas subjacentes dos serviços LDR disponíveis são corrigidos. Certifique-se de que o componente HTTP dos serviços LDR esteja online e funcionando normalmente.</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>
CCES	Sessões recebidas - estabelecidas	CLB	<p>Este alarme é acionado se houver 20.000 ou mais sessões HTTP atualmente ativas (abertas) no Gateway Node. Se um cliente tiver muitas conexões, você poderá ver falhas de conexão. Você deve reduzir o workload.</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 esse alarme atingir o limite de 90%, um aviso será exibido no Painel no Gerenciador de Grade. Você deve executar um procedimento de expansão para adicionar novos nós de storage o mais rápido possível. Expanda sua gradeConsulte .</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>
CLBA	Estado CLB	CLB	<p>Se um alarme for acionado, selecione support Tools Grid topology, em seguida, selecione site grid node CLB Overview Main e CLB Alarmes Main para determinar a causa do alarme e solucionar o problema.</p> <p>Se o problema persistir, entre em Contato com o suporte técnico.</p>
CLBE	Estado CLB	CLB	<p>Se o valor do Estado CLB for Standby (em espera), continue a monitorizar a situação e, se o problema persistir, contacte o suporte técnico.</p> <p>Se o estado estiver Offline e não houver problemas conhecidos de hardware do servidor (por exemplo, o servidor está desconetado) ou tempo de inatividade programado, reinicie o serviço. Se o problema persistir, entre em Contato com o suporte técnico.</p>

Código	Nome	Serviço	Ação recomendada
CMNA	Estado CMN	CMN	<p>Se o valor do Status do CMN for erro, selecione SUPPORT Tools Grid topology, 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>
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>

Código	Nome	Serviço	Ação recomendada
DNST	Estado DNS	SSM	Após a conclusão da instalação, um alarme DNST é acionado no serviço SSM. Depois que o DNS é configurado e as novas informações do servidor atingem todos os nós da grade, o alarme é cancelado.
ECCD	Fragmentos corrompidos detetados	LDR	<p>Um alarme é acionado quando o processo de verificação em segundo plano deteta um fragmento codificado de apagamento corrompido. 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 codificado de 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 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 apagar dados de objetos codificados 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 ao protocolo HTTP para todo o tráfego LDR, incluindo S3, Swift e outro tráfego interno de StorageGRID. Um alarme indica que ocorreu uma das seguintes situações:</p> <ul style="list-style-type: none"> • O protocolo 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 protocolo HTTP estiver offline, coloque-o online. Verifique se o atributo Auto-Start HTTP está ativado.</p> <p>Se o protocolo HTTP permanecer off-line, 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	Deteção 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 redefinir 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 diminuir. 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 site grid node CMN Grid Tasks Overview Main. A mensagem de tarefa de grade exibe informações sobre o erro (por exemplo, "verificação falhou no nó 12130011").</p> <p>Depois de investigar e corrigir o problema, reinicie a tarefa de grade. Selecione SUPPORT Tools Grid topology. Em seguida, selecione site grid node CMN Grid Tasks Configuration Main e selecione Actions Run.</p> <p>Se o valor de Status para uma tarefa de grade que está sendo cancelada for erro, tente abortar 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 style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Para redefinir contagens de eventos, você deve ter a permissão 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 software SANtricity indicar que há um problema de "precisa 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 software SANtricity, verifique outros componentes do dispositivo para isolar o problema.</p>
SSMA	Estado SSM	SSM	<p>Se o valor do Status SSM for erro, selecione SUPPORT Tools Grid topology e, em seguida, selecione site grid node SSM Overview Main e SSM Overview Alarms 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 Grid topology (SUPORTE* Ferramentas topologia da grelha). 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 site grid node SSM Serviços Visão geral Principal. Quando o status de um serviço é mostrado como não em execução, seu estado é administrativamente inativo. O status do serviço pode ser listado como não em execução pelos seguintes motivos:</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	Se o valor de espaço disponível ficar muito baixo (consulte limiares de alarme), ele precisa ser investigado se há arquivos de log crescendo fora de proporção, ou objetos ocupando muito espaço em disco (veja limiares de alarme) que precisam ser reduzidos ou excluídos. Se o problema persistir, entre em Contato com o suporte técnico.
VMST	Estado	SSM	Um alarme é acionado se o valor de Status para o volume montado for desconhecido. Um valor desconhecido ou Offline pode indicar que o volume não pode ser montado ou acessado devido a um problema com o dispositivo de armazenamento subjacente.
VPRI	Prioridade de verificação	BLDR, BARC	Por padrão, o valor da prioridade de verificação é adaptável. Se a prioridade de verificação estiver definida como alta, um alarme é acionado porque a verificação do armazenamento pode retardar as operações normais do serviço.
VSTU	Estado Verificação Objeto	ERRO	Selecione SUPPORT Tools Grid topology . Em seguida, selecione site grid node LDR Storage Overview Main . Verifique se existem sinais de erros no sistema operativo ou no sistema de ficheiros. Se o valor do Status de Verificação de Objeto for erro desconhecido, ele geralmente indica um problema de hardware ou sistema de arquivos de baixo nível (erro de e/S) que impede que a tarefa de Verificação de armazenamento acesse conteúdo armazenado. Entre em Contato com o suporte técnico.

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

Alarmes que geram notificações SNMP (sistema legado)

A tabela a seguir lista os alarmes legados que geram notificações SNMP. Ao contrário dos alertas, nem todos os alarmes geram notificações SNMP. Apenas os alarmes listados geram notificações SNMP e apenas com a gravidade indicada ou superior.



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	Gravidade
ACMS	Serviços de metadados disponíveis	Crítico
AITE	Recuperar Estado	Menor
AITU	Recuperar Estado	Maior
AMQS	Mensagens de auditoria enfileiradas	Aviso
AOTE	Estado da loja	Menor
AOTU	Estado da loja	Maior
AROQ	Objetos em fila de espera	Menor
ARRF	Falhas de solicitação	Maior
ARRV	Falhas de verificação	Maior
ARVF	Falhas de armazenamento	Maior
ASXP	Compartilhamentos de auditoria	Menor
AUMA	Estado AMS	Menor
AUXS	Estado exportação Auditoria	Menor
BTOF	Desvio	Aviso

Código	Nome	Gravidade
CAHP	Porcentagem de uso do Java Heap	Maior
CAQH	Número de destinos disponíveis	Aviso
CASA	Estado do armazenamento de dados	Maior
CDLP	Espaço usado (porcentagem)	Maior
CLBE	Estado CLB	Crítico
DNST	Estado DNS	Crítico
ECST	Estado de verificação	Maior
HSTE	Estado HTTP	Maior
HTAS	Auto-Iniciar HTTP	Aviso
PERDIDO	Objetos perdidos	Maior
MINQ	Notificações de e-mail na fila	Aviso
MIN	Estado das notificações por e-mail	Menor
NANG	Configuração de negociação automática de rede	Aviso
NDUP	Configuração Duplex de rede	Menor
NLNK	Detecção de ligação de rede	Menor
NRER	Receber erros	Aviso
VELOCIDADE MÁXIMA	Velocidade	Aviso
NTER	Transmitir erros	Aviso
NTFQ	Desvio de frequência NTP	Menor
NTLK	Bloqueio NTP	Menor
NTOF	Desvio horário NTP	Menor
NTSJ	Jitter de fonte de tempo escolhido	Menor

Código	Nome	Gravidade
NTSU	Estado NTP	Maior
OPST	Estado geral da alimentação	Maior
ORSU	Estado replicação saída	Aviso
PSAS	Estado da fonte de alimentação A.	Maior
PSB	Estado da fonte de alimentação B.	Maior
RDTE	Estado do Tivoli Storage Manager	Aviso
RDTU	Status do Tivoli Storage Manager	Maior
SAVP	Espaço utilizável total (percentagem)	Aviso
SHLH	Saúde	Aviso
SLSA	Média de carga da CPU	Aviso
SMTT	Total de eventos	Aviso
SNST	Estado	
SOSS	Estado do sistema operativo de armazenamento	Aviso
SSTS	Estado de armazenamento	Aviso
SVST	Estado	Aviso
TMEM	Memória instalada	Menor
UMEM	Memória disponível	Menor
VMST	Estado	Menor
VPRI	Prioridade de verificação	Aviso
VSTU	Estado Verificação Objeto	Aviso

Referência de ficheiros de registo

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.

Para acessar os logs, você pode coletar arquivos de log e dados do sistema de um ou mais nós como um único arquivo de log (**SUPPORT Tools Logs**). 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.

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

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

Localização do arquivo	Descrição
instale	Gdu-server e instalar logs.
lumberjack.log	Depurar mensagens relacionadas à coleção de logs.
Lambda-árbitro	Logs relacionados à solicitação de proxy S3 Select.
Métricas	Logs de serviço para Grafana, Jaeger, nó exportador e Prometheus.
miscd	Registos de acesso e erro incorretos.
mysql	A configuração do banco de dados MariaDB e logs relacionados.
rede	Logs gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos de configuração do balanceador de carga e logs. Também inclui logs de tráfego do Grid Manager e do Tenant Manager.
nginx-gw	Arquivos de configuração do balanceador de carga e logs.
ntp	Ficheiro de configuração NTP e registos.
so	Arquivo de estado de nó e grade, incluindo serviços pid.
outros	Arquivos de log sob /var/local/log que não são coletados em outras pastas.
perf	Informações de desempenho para CPU, rede e e/S de disco
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.
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.

Informações relacionadas

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


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
<code>/var/local/log/bycast.log</code>	O arquivo primário de solução de problemas do StorageGRID. Selecione SUPPORT Tools Grid topology . Em seguida, selecione Site Node SSM Eventos .	Todos os nós
<code>/var/local/log/bycast-err.log</code>	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
<code>/var/local/core/</code>	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.  O arquivo <code>/var/local/core/kexec_cmd</code> geralmente existe nos nós do dispositivo e não indica um erro.	Todos os nós

Logs do Server Manager

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

Logs para serviços 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/clb.errlog	Informações de erro para o serviço CLB. Nota: o serviço CLB está obsoleto.	Nós de gateway
/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

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

Nome do ficheiro	Notas	Encontrado em
/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

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

Nome do ficheiro	Notas	Encontrado em
/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

Informações relacionadas

[Sobre o bycast.log](#)

[Use 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
/var/local/log/expansion-progress.log	Criado durante operações de expansão. Contém um Registro dos eventos de expansão.	Nós de storage
/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

Nome do ficheiro	Notas	Encontrado em
/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. O arquivo <code>mysql.err</code> captura erros de banco de dados e eventos, como startups e paradas. O arquivo <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
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/	<code>/var/local/log/ntp.log</code> Contém o arquivo de log para mensagens de erro NTP. O <code>/var/lib/ntp/var/log/ntpstats/</code> diretório contém estatísticas de tempo NTP. <code>loopstats</code> registra informações estatísticas de filtro de loop. <code>peerstats</code> registra informações estatísticas de pares.	Todos os nós

Categoria	Nome do ficheiro	Notas	Encontrado em
Samba	<code>/var/local/log/samba/</code>	O diretório de log do Samba inclui um arquivo de log para cada processo Samba (SMB, nmb e winbind) e cada nome de host/IP do cliente.	Admin Node configurado para exportar o compartilhamento de auditoria por CIFS

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.UUUUUUUUUUUUUUUU)
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

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

Número de erro	Código de erro	Significado
027	EFBIG	Ficheiro demasiado grande
028	ENOSPC	Nenhum espaço restante no dispositivo
029	ESPIPE	Procura ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Demasiados links
032	EPIPE	Tubo quebrado
033	EDOM	Argumento de matemática fora de domínio do func
034	ERANGE	Resultado matemático não representável
035	EDEADLK	O bloqueio de recursos ocorreria
036	ENAMETOOLONG	Nome do ficheiro demasiado longo
037	ENOLCK	Não existem bloqueios de registo disponíveis
038	ENOSYS	Função não implementada
039	ENOTEMPTY	O diretório não está vazio
040	ELOOP	Muitos links simbólicos encontrados
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido
044	ECHRNG	Número do canal fora do intervalo
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

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

Número de erro	Código de erro	Significado
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de Multihop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	E_OVERFLOW	Valor demasiado grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em mau estado
078	EREMCHG	Endereço remoto alterado
079	ELIBACC	Não é possível acessar uma biblioteca compartilhada necessária
080	ELIBBAD	Acessando uma biblioteca compartilhada corrompida
081	ELIBSCN	
082	ELIBMAX	Tentando vincular em muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada do sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro no tubo de fluxos
087	EUSERS	Demasiados utilizadores
088	ENOTSOCK	Funcionamento da tomada sem tomada
089	EDESTADDRREQ	Endereço de destino obrigatório
090	EMSGSIZE	Mensagem demasiado longa

Número de erro	Código de erro	Significado
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 causou interrupção da ligação
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
108	ESHUTDOWN	Não é possível enviar após o encerramento do terminal de transporte
109	ETOOMANYREFS	Demasiadas referências: Não é possível unir
110	ETIMEDOUT	Tempo de ligação esgotado
111	ECONNREFUSED	Ligação recusada

Número de erro	Código de erro	Significado
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
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

Expanda sua grade

Expanda sua grade: Visão geral

Use estas instruções para expandir a capacidade ou as funcionalidades do sistema StorageGRID sem interromper as operações do sistema.

Sobre estas instruções

Essas instruções descrevem como executar uma expansão do StorageGRID para adicionar volumes de storage a nós de storage, novos nós de grade a um local existente ou a um local novo inteiro.

Estas instruções destinam-se ao pessoal técnico responsável pela configuração e suporte do sistema StorageGRID após a instalação.

Visão geral do procedimento de expansão

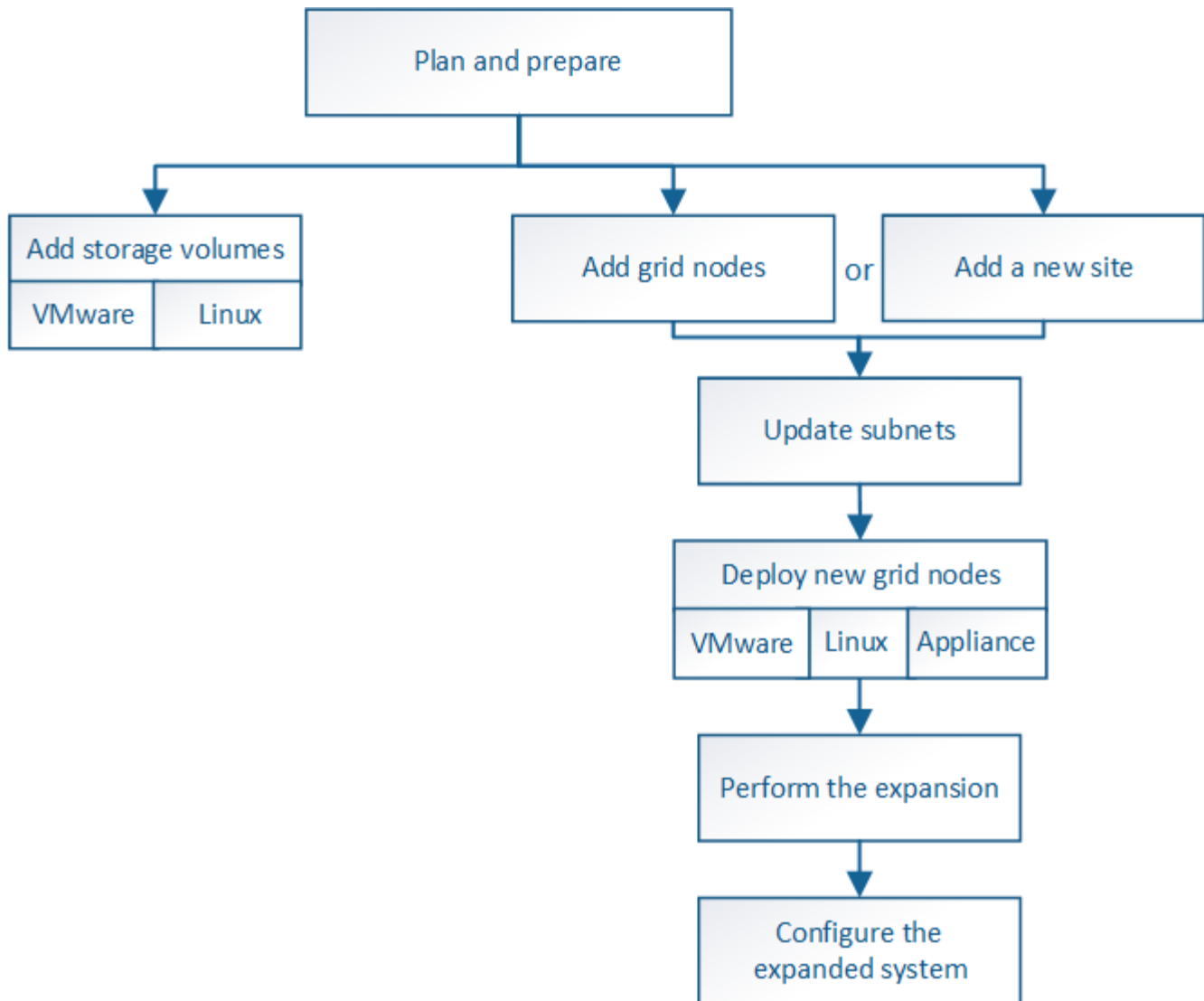
A razão pela qual você está executando a expansão determina quantos novos nós de cada tipo você deve adicionar e o local desses novos nós. Por exemplo, há requisitos de nó diferentes se você estiver executando uma expansão para aumentar a capacidade de storage, adicionar capacidade de metadados ou adicionar redundância ou novos recursos.

Como mostrado no diagrama de fluxo de trabalho, as etapas para executar uma expansão dependem da adição de volumes de storage a um nó de storage, da adição de novos nós a um site existente ou da adição de um novo local. Em todos os casos, você pode executar a expansão sem interromper a operação do sistema atual.

As etapas para adicionar nós também dependem se você está adicionando dispositivos StorageGRID ou hosts executando VMware ou Linux.



"Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Utilize o "[Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)](#)" para obter uma lista de versões suportadas.



Planeje a expansão do StorageGRID

Adicionar capacidade de armazenamento

Diretrizes para adicionar capacidade de objeto

Você pode expandir a capacidade de storage de objetos do seu sistema StorageGRID adicionando volumes de storage a nós de storage existentes ou adicionando novos nós de storage a locais existentes. Você precisa adicionar capacidade de storage de forma que atenda aos requisitos da política de gerenciamento do ciclo de vida das informações (ILM).

Diretrizes para adicionar volumes de armazenamento

Antes de adicionar volumes de storage a nós de storage existentes, consulte as diretrizes e limitações a seguir:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando adicionar volumes de storage para aumentar o storage disponível para objetos replicados ou codificados por apagamento. Consulte as instruções para [gerenciamento de objetos com gerenciamento do ciclo de vida das](#)

informações.

- Você não pode aumentar a capacidade de metadados do sistema adicionando volumes de storage porque os metadados de objetos são armazenados apenas no volume 0.
- Cada nó de storage baseado em software pode dar suporte a um máximo de 16 volumes de storage. Se você precisar adicionar capacidade além disso, precisará adicionar novos nós de storage.
- Você pode adicionar uma ou duas gavetas de expansão a cada dispositivo SG6060 ou SG6060X. Cada compartimento de expansão adiciona 16 volumes de storage. Com ambas as gavetas de expansão instaladas, o SG6060 e o SG6060X podem dar suporte a um total de 48 volumes de storage.
- Não é possível adicionar volumes de armazenamento a qualquer outro dispositivo de armazenamento.
- Não é possível aumentar o tamanho de um volume de armazenamento existente.
- Não é possível adicionar volumes de armazenamento a um nó de armazenamento ao mesmo tempo em que está a efetuar uma atualização do sistema, uma operação de recuperação ou outra expansão.

Depois de decidir adicionar volumes de storage e determinar quais nós de storage você deve expandir para atender à política de ILM, siga as instruções para seu tipo de nó de storage:

- Para adicionar uma ou duas gavetas de expansão a um dispositivo de storage SG6060 ou SG6060X, vá para [Adicione o compartimento de expansão ao SG6060 ou SG6060X implantados](#).
- Para um nó baseado em software, siga as instruções para [Adição de volumes de storage aos nós de storage](#).

Diretrizes para a adição de nós de storage

Antes de adicionar nós de storage a sites existentes, consulte as diretrizes e limitações a seguir:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando adicionar nós de storage para aumentar o storage disponível para objetos replicados ou codificados por apagamento. Consulte as instruções para [gerenciamento de objetos com gerenciamento do ciclo de vida das informações](#).
- Você não deve adicionar mais de 10 nós de storage em um único procedimento de expansão.
- Você pode adicionar nós de storage a mais de um local em um único procedimento de expansão.
- Você pode adicionar nós de storage e outros tipos de nós em um único procedimento de expansão.
- Antes de iniciar o procedimento de expansão, deve confirmar se todas as operações de reparação de dados efetuadas como parte de uma recuperação estão concluídas. [Verifique os trabalhos de reparação de dados](#)Consulte .
- Se você precisar remover nós de storage antes ou depois de executar uma expansão, não deverá desativar mais de 10 nós de storage em um único procedimento de nó de compactação.

Diretrizes para o serviço ADC em nós de storage

Ao configurar a expansão, você deve escolher se deseja incluir o serviço controlador de domínio administrativo (ADC) em cada novo nó de armazenamento. O serviço ADC mantém o controle da localização e disponibilidade dos serviços da grade.

- O sistema StorageGRID requer que a [Quórum de serviços ADC](#) esteja disponível em cada local e em todos os momentos.
- Pelo menos três nós de storage em cada local devem incluir o serviço ADC.
- Adicionar o serviço ADC a cada nó de armazenamento não é recomendado. Incluir muitos serviços ADC pode causar lentidão devido ao aumento da quantidade de comunicação entre nós.

- Uma única grade não deve ter mais de 48 nós de storage com o serviço ADC. Isso equivale a 16 sites com três serviços ADC em cada local.
- Em geral, quando você seleciona a configuração **ADC Service** para um novo nó, você deve selecionar **Automatic**. Selecione **Sim** somente se o novo nó substituir outro nó de armazenamento que inclua o serviço ADC. Como você não pode desativar um nó de armazenamento se houver poucos serviços ADC, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido.
- Você não pode adicionar o serviço ADC a um nó depois que ele é implantado.

Adicione capacidade de storage para objetos replicados

Se a política de gerenciamento do ciclo de vida das informações (ILM) da implantação incluir uma regra que crie cópias replicadas de objetos, você deverá considerar quanto storage adicionar e onde adicionar os novos volumes de storage ou nós de storage.

Para obter orientação sobre onde adicionar armazenamento adicional, examine as regras do ILM que criam cópias replicadas. Se as regras do ILM criarem duas ou mais cópias de objetos, Planeje adicionar storage em cada local em que as cópias de objetos forem feitas. Como um exemplo simples, se você tiver uma grade de dois locais e uma regra ILM que crie uma cópia de objeto em cada local, você deve adicionar armazenamento a cada local para aumentar a capacidade geral de objeto da grade. Consulte as instruções para [gerenciamento de objetos com gerenciamento do ciclo de vida das informações](#).

Por motivos de desempenho, você deve tentar manter a capacidade de storage e o poder de computação equilibrados em todos os locais. Portanto, para este exemplo, você deve adicionar o mesmo número de nós de storage a cada local ou volumes de storage adicionais em cada local.

Se você tiver uma política de ILM mais complexa que inclua regras que coloquem objetos em locais diferentes com base em critérios como nome do bucket ou regras que alterem os locais do objeto ao longo do tempo, sua análise de onde o armazenamento é necessário para a expansão será semelhante, mas mais complexa.

Traçar a rapidez com que a capacidade geral de armazenamento está sendo consumida pode ajudá-lo a entender quanto armazenamento adicionar na expansão e quando o espaço de armazenamento adicional será necessário. Você pode usar o Gerenciador de Grade para monitorar e mapear a capacidade de armazenamento, conforme descrito nas instruções para [Monitoramento e solução de problemas do StorageGRID](#).

Ao Planejar o momento de uma expansão, lembre-se de considerar quanto tempo pode levar para adquirir e instalar armazenamento adicional.

Adicionar capacidade de storage para objetos codificados por apagamento

Se a política de ILM incluir uma regra que faça cópias codificadas por apagamento, você deve Planejar onde adicionar um novo storage e quando adicionar um novo storage. A quantidade de armazenamento que você adiciona e o tempo da adição podem afetar a capacidade de armazenamento utilizável da grade.

A primeira etapa no Planejamento de uma expansão de storage é examinar as regras da política de ILM que criam objetos codificados por apagamento. Como o StorageGRID cria fragmentos $k-m$ para cada objeto codificado de apagamento e armazena cada fragmento em um nó de storage diferente, você deve garantir que pelo menos os nós de storage $k-m$ tenham espaço para novos dados codificados de apagamento após a expansão. Se o perfil de codificação de apagamento fornecer proteção contra perda de site, você precisará adicionar storage a cada local. [Gerenciar objetos com ILM](#)Consulte .

O número de nós que você precisa adicionar também depende de quão cheios os nós existentes estão quando você executa a expansão.

Recomendação geral para adicionar capacidade de storage para objetos codificados por apagamento

Se você quiser evitar cálculos detalhados, pode adicionar dois nós de storage por local quando os nós de storage existentes atingirem 70% de capacidade.

Esta recomendação geral fornece resultados razoáveis em uma ampla variedade de esquemas de codificação de apagamento para grades de um único local e para grades onde a codificação de apagamento fornece proteção contra perda de site.

Para entender melhor os fatores que levam a esta recomendação ou para desenvolver um plano mais preciso para o seu site, revise a próxima seção. Para obter uma recomendação personalizada otimizada para a sua situação, entre em Contato com o representante da sua conta NetApp.

Calcule o número de nós de storage de expansão a serem adicionados para objetos codificados por apagamento

Para otimizar a forma como você expande uma implantação que armazena objetos codificados por apagamento, considere muitos fatores:

- Esquema de codificação de apagamento em uso
- Características do pool de storage usado para codificação de apagamento, incluindo o número de nós em cada local e a quantidade de espaço livre em cada nó
- Se a grade foi expandida anteriormente (porque a quantidade de espaço livre por nó de storage pode não ser aproximadamente a mesma em todos os nós)
- Natureza exata da política ILM, como se as regras ILM fazem objetos replicados e codificados por apagamento

Os exemplos a seguir podem ajudar você a entender o impacto do esquema de codificação de apagamento, o número de nós no pool de storage e a quantidade de espaço livre em cada nó.

Considerações semelhantes afetam os cálculos de uma política de ILM que armazena dados replicados e codificados por apagamento e os cálculos de uma grade que foi expandida anteriormente.



Os exemplos nesta seção representam as práticas recomendadas para adicionar capacidade de storage a um sistema StorageGRID. Se você não conseguir adicionar o número recomendado de nós, talvez seja necessário executar o procedimento de rebalanceamento EC para permitir que objetos codificados de apagamento adicionais sejam armazenados. [Rebalancear os dados codificados por apagamento](#) Consulte .

Exemplo 1: Expanda a grade de um site que usa codificação de apagamento 2-1

Este exemplo mostra como expandir uma grade simples que inclui apenas três nós de storage.



Este exemplo usa apenas três nós de storage para simplificar. No entanto, o uso de apenas três nós de storage não é recomendado: Uma grade de produção real deve usar um mínimo de 1 nós de storage para redundância, o que equivale a quatro nós de storage (2-1-1) para este exemplo.

Assuma o seguinte:

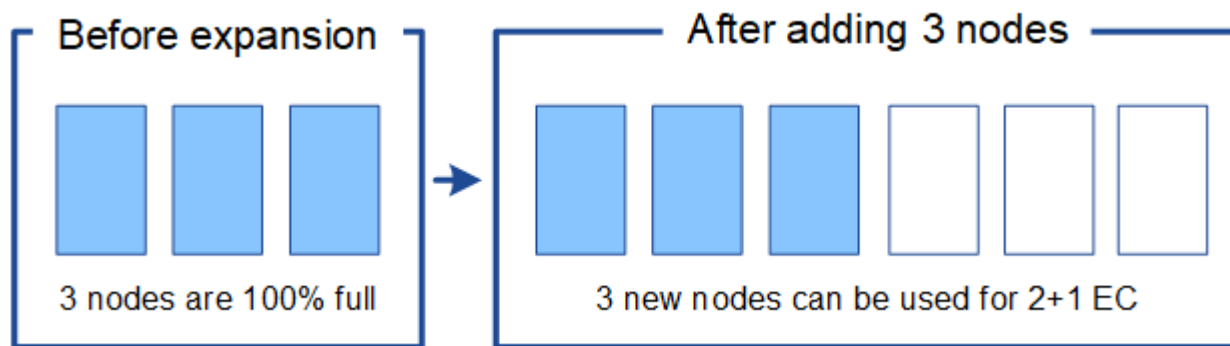
- Todos os dados são armazenados usando o esquema de codificação de apagamento 2-1. Com o esquema de codificação de apagamento 2-1, cada objeto é armazenado como três fragmentos e cada fragmento é salvo em um nó de storage diferente.
- Você tem um local com três nós de storage. Cada nó de storage tem uma capacidade total de 100 TB.
- Você deseja expandir adicionando novos nós de storage de 100 TB.
- No momento, você deseja equilibrar os dados codificados por apagamento entre os nós antigos e os novos.

Você tem várias opções, com base em quão cheios os nós de storage estão quando você executa a expansão.

- **Adicione três nós de storage de 100 TB quando os nós existentes estiverem 100% cheios**

Neste exemplo, os nós existentes estão 100% cheios. Como não há capacidade livre, você precisa adicionar imediatamente três nós para continuar a codificação de apagamento em mais de 1 hora por dia, 2 dias por semana.

Depois que a expansão for concluída, quando os objetos forem codificados para apagamento, todos os fragmentos serão colocados nos novos nós.

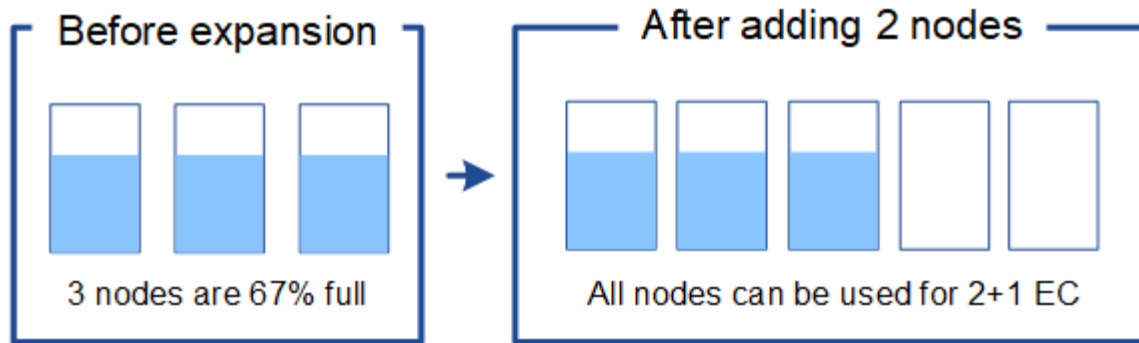


Essa expansão adiciona nós $k m$. A adição de quatro nós é recomendada para redundância. Se você adicionar somente nós de armazenamento de expansão $k m$ quando os nós existentes estiverem 100% cheios, todos os novos objetos serão armazenados nos nós de expansão. Se algum dos novos nós ficar indisponível, mesmo temporariamente, o StorageGRID não poderá atender aos requisitos do ILM.

- **Adicione dois nós de storage de 100 TB, quando os nós de storage existentes estiverem 67% completos**

Neste exemplo, os nós existentes estão 67% cheios. Como há 100 TB de capacidade livre nos nós existentes (33 TB por nó), você só precisa adicionar dois nós se você executar a expansão agora.

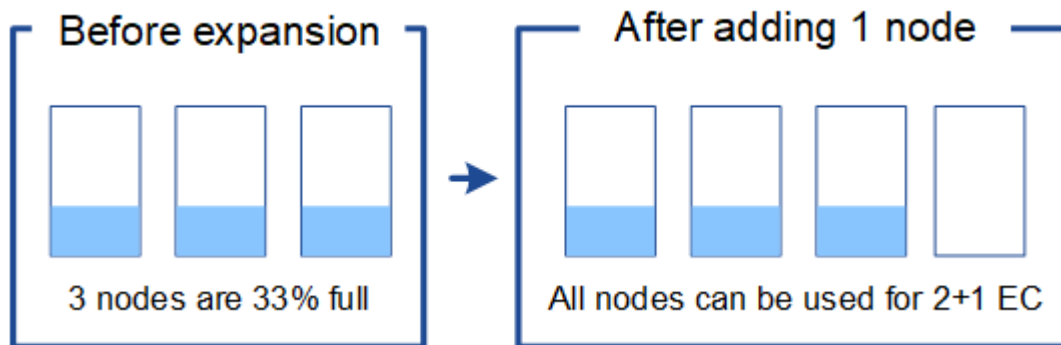
A adição de 200 TB de capacidade adicional permite que você continue a codificação de apagamento de mais de 1 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.



- Adicione um nó de storage de 100 TB quando os nós de storage existentes estiverem 33% cheios

Neste exemplo, os nós existentes estão 33% cheios. Como há 200 TB de capacidade livre nos nós existentes (67 TB por nó), você só precisa adicionar um nó se você executar a expansão agora.

A adição de 100 TB de capacidade adicional permite que você continue 2 a codificação de apagamento de mais de 1 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.



Exemplo 2: Expanda a grade de três locais que usa codificação de apagamento 6-3

Este exemplo mostra como desenvolver um plano de expansão para uma grade multi-site que tenha um esquema de codificação de apagamento com um número maior de fragmentos. Apesar das diferenças entre esses exemplos, o plano de expansão recomendado é muito semelhante.

Assuma o seguinte:

- Todos os dados são armazenados usando o esquema de codificação de apagamento 6-3. Com o esquema de codificação de apagamento 6-3, cada objeto é armazenado como 9 fragmentos e cada fragmento é salvo em um nó de storage diferente.
- Você tem três locais e cada local tem quatro nós de storage (12 nós no total). Cada nó tem uma capacidade total de 100 TB.
- Você deseja expandir adicionando novos nós de storage de 100 TB.
- No momento, você deseja equilibrar os dados codificados por apagamento entre os nós antigos e os novos.

Você tem várias opções, com base em quão cheios os nós de storage estão quando você executa a expansão.

- Adicione nove nós de storage de 100 TB (três por local), quando os nós existentes estiverem 100% completos

Neste exemplo, os 12 nós existentes estão 100% cheios. Como não há capacidade livre, você precisa adicionar imediatamente nove nós (900 TB de capacidade adicional) para continuar a codificação de apagamento 6-3.

Depois que a expansão for concluída, quando os objetos forem codificados para apagamento, todos os fragmentos serão colocados nos novos nós.



Essa expansão adiciona nós $k m$. A adição de 12 nós (quatro por local) é recomendada para redundância. Se você adicionar somente nós de armazenamento de expansão $k m$ quando os nós existentes estiverem 100% cheios, todos os novos objetos serão armazenados nos nós de expansão. Se algum dos novos nós ficar indisponível, mesmo temporariamente, o StorageGRID não poderá atender aos requisitos do ILM.

- **Adicione seis nós de storage de 100 TB (dois por local), quando os nós existentes estiverem 75% completos**

Neste exemplo, os 12 nós existentes estão 75% cheios. Como há 300 TB de capacidade livre (25 TB por nó), você só precisa adicionar seis nós se você executar a expansão agora. Você adicionaria dois nós a cada um dos três locais.

A adição de 600 TB de capacidade de storage permitirá que você continue a codificação de apagamento de mais de 3 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.

- **Adicione três nós de storage de 100 TB (um por local), quando os nós existentes estiverem 50% completos**

Neste exemplo, os 12 nós existentes estão 50% cheios. Como há 600 TB de capacidade livre (50 TB por nó), você só precisa adicionar três nós se você executar a expansão agora. Você adicionaria um nó a cada um dos três locais.

A adição de 300 TB de capacidade de storage permitirá que você continue a codificação de apagamento de mais de 3 TB e, eventualmente, equilibrar os dados codificados por apagamento em todos os nós.

Considerações para rebalanceamento de dados codificados por apagamento

Se você estiver executando uma expansão para adicionar nós de storage e sua política de ILM incluir uma ou mais regras de ILM para apagar dados de código, talvez seja necessário executar o procedimento de rebalanceamento de EC após a conclusão da expansão.

Por exemplo, se você não puder adicionar o número recomendado de nós de storage para o esquema de codificação de apagamento que você está usando, talvez seja necessário executar o procedimento de rebalanceamento de EC para permitir que objetos codificados de apagamento adicionais sejam armazenados.

Depois de analisar estas considerações, execute a expansão e, em seguida, vá para [Rebalancear os dados codificados por apagamento após adicionar nós de storage](#) para executar o procedimento.

O que é o reequilíbrio CE?

O rebalanceamento EC é um procedimento StorageGRID que pode ser necessário após uma expansão do nó de storage. O procedimento é executado como um script de linha de comando a partir do nó de administração principal. Ao executar o procedimento de rebalancear, o StorageGRID redistribui fragmentos codificados por apagamento entre os nós de storage existentes e recém-expandidos em um local.

O procedimento de reequilíbrio CE:

- Move apenas dados de objetos codificados por apagamento. Ele não move dados de objetos replicados.
- Redistribui os dados em um local. Ele não move dados entre sites.
- Redistribui dados entre todos os nós de storage em um local. Ele não redistribui dados dentro de volumes de storage.
- Não considera o uso de dados replicados em cada nó de storage ao determinar para onde mover dados codificados por apagamento

Quando o procedimento de reequilíbrio CE estiver concluído:

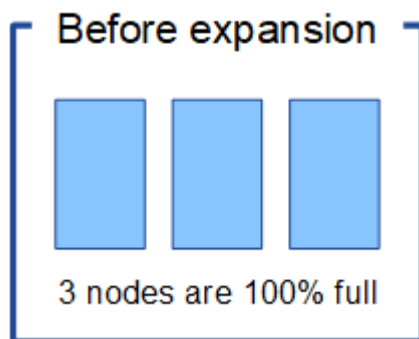
- Os dados codificados por apagamento são movidos de nós de storage com menos espaço disponível para nós de storage com mais espaço disponível.
- Os valores usados (%) podem permanecer diferentes entre nós de storage porque o procedimento de rebalanceamento de EC não move cópias de objeto replicadas.
- A proteção de dados de objetos codificados por apagamento não será alterada.

Quando o procedimento de reequilíbrio EC está em execução, o desempenho das operações ILM e das operações dos clientes S3 e Swift provavelmente serão impactados. Por esse motivo, você só deve executar esse procedimento em casos limitados.

Quando não realizar o rebalanceamento EC

Como exemplo de quando você não precisa realizar um rebalanceamento EC, considere o seguinte:

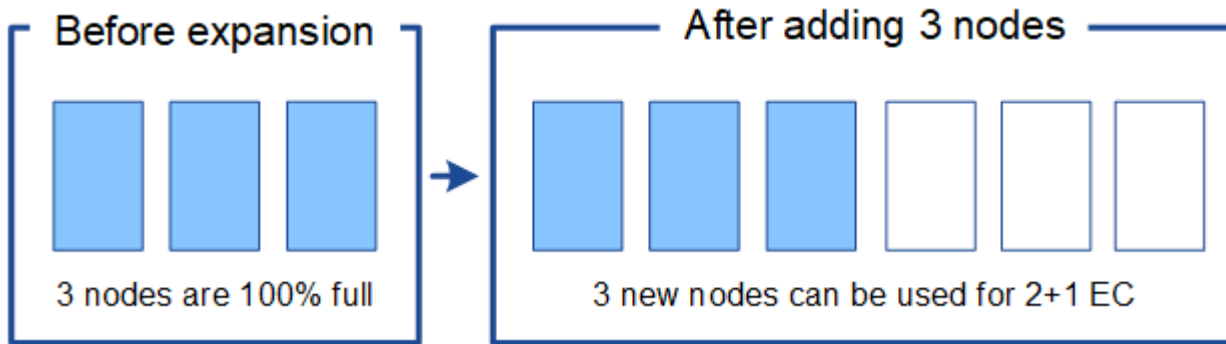
- O StorageGRID é executado em um único local, que contém três nós de storage.
- A política ILM usa uma regra de codificação de apagamento de mais de 2 1 para todos os objetos com mais de 1,0 MB e uma regra de replicação de 2 cópias para objetos menores.
- Todos os nós de storage ficaram completamente cheios e o alerta **armazenamento de objetos baixos** foi acionado no nível de gravidade maior. A ação recomendada é executar um procedimento de expansão para adicionar nós de storage.



Para expandir o site neste exemplo, é recomendável adicionar três ou mais nós de storage novos. O StorageGRID precisa de três nós de storage para codificação de apagamento em mais de 1 hora por dia, 2 dias por semana, para que ele possa colocar os dois fragmentos de dados e um fragmento de paridade em nós diferentes.

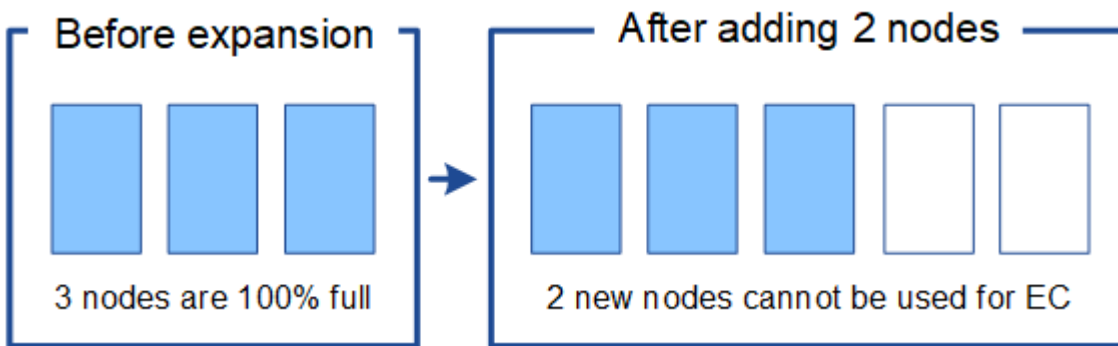
Depois de adicionar os três nós de storage, os nós de storage originais permanecem cheios, mas os objetos podem continuar sendo ingeridos no 1 esquema de codificação de apagamento de mais de 2% nos novos nós. A execução do procedimento de reequilíbrio EC não é recomendada para este caso: A execução do

procedimento diminuirá temporariamente o desempenho, o que pode afetar as operações do cliente.

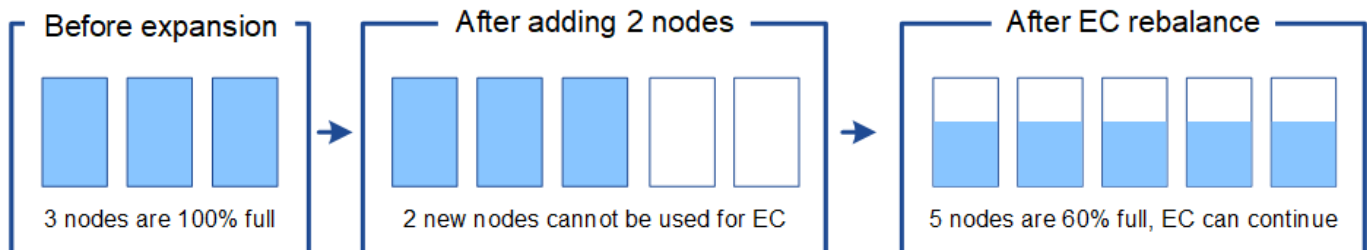


Quando realizar o rebalanceamento EC

Como exemplo de quando você deve executar o procedimento de rebalanceamento de EC, considere o mesmo exemplo, mas suponha que você só pode adicionar dois nós de storage. Como a codificação de apagamento de mais de 2 vezes por dia requer pelo menos 1 nós de storage, os novos nós não podem ser usados para dados codificados por apagamento.



Para resolver esse problema e usar os novos nós de storage, é possível executar o procedimento de rebalanceamento de EC. Quando esse procedimento é executado, o StorageGRID redistribui dados codificados de apagamento e fragmentos de paridade entre todos os nós de storage no local. Neste exemplo, quando o procedimento de rebalanceamento do EC estiver concluído, todos os cinco nós agora estão apenas 60% cheios e os objetos podem continuar a ser ingeridos no 2 esquema de codificação de apagamento de mais de 1 anos em todos os nós de storage.



Requisitos para o reequilíbrio CE

Em geral, só deve executar o procedimento de reequilíbrio CE em casos limitados. Especificamente, você deve realizar o rebalanceamento EC somente se todas as seguintes afirmações forem verdadeiras:

- Você usa codificação de apagamento para seus dados de objeto.

- O alerta **Low Object Storage** foi acionado para um ou mais nós de storage em um local, indicando que os nós estão 80% ou mais cheios.
- Não é possível adicionar o número recomendado de novos nós de storage para o esquema de codificação de apagamento em uso. [Adicionar capacidade de storage para objetos codificados por apagamento](#) Consulte .
- Seus clientes S3 e Swift podem tolerar um desempenho inferior para suas operações de gravação e leitura enquanto o procedimento EC Rebalanceance está sendo executado.

Como o procedimento EC Rebalanceance interage com outras tarefas de manutenção

Não é possível executar determinados procedimentos de manutenção ao mesmo tempo que está a executar o procedimento EC Rebalanceance.

Procedimento	Permitido durante o procedimento de reequilíbrio CE?
Procedimentos adicionais de reequilíbrio da CE	Não Só é possível executar um procedimento de rebalanceamento EC de cada vez.
Procedimento de desativação Trabalho de reparação de dados EC	Não <ul style="list-style-type: none"> • É impedido de iniciar um procedimento de desativação ou uma reparação de dados EC enquanto o procedimento de reequilíbrio EC está em execução. • É impedido de iniciar o procedimento de rebalanceamento EC enquanto um procedimento de desativação do nó de storage ou um reparo de dados EC estiver em execução.
Procedimento de expansão	Não Se você precisar adicionar novos nós de storage em uma expansão, aguarde para executar o procedimento de rebalanceamento do EC até que você tenha adicionado todos os novos nós. Se um procedimento de rebalanceamento do EC estiver em andamento quando você adicionar novos nós de storage, os dados não serão movidos para esses nós.
Procedimento de atualização	Não Se você precisar atualizar o software StorageGRID, execute o procedimento de atualização antes ou depois de executar o procedimento de rebalanceamento EC. Conforme necessário, você pode encerrar o procedimento EC Rebalanceance para realizar uma atualização de software.

Procedimento	Permitido durante o procedimento de reequilíbrio CE?
Procedimento de clone de nó do dispositivo	Não Se você precisar clonar um nó de storage de dispositivo, aguarde para executar o procedimento de rebalanceamento do EC até que você tenha adicionado o novo nó. Se um procedimento de rebalanceamento do EC estiver em andamento quando você adicionar novos nós de storage, os dados não serão movidos para esses nós.
Procedimento de correção	Sim. Você pode aplicar um hotfix do StorageGRID enquanto o procedimento EC Rebalanceance estiver sendo executado.
Outros procedimentos de manutenção	Não Você deve terminar o procedimento EC Rebalanceance antes de executar outros procedimentos de manutenção.

Como o procedimento EC Rebalanceance interage com o ILM

Enquanto o procedimento de rebalanceamento EC estiver em execução, evite fazer alterações no ILM que possam alterar o local dos objetos codificados por apagamento existentes. Por exemplo, não comece a usar uma regra ILM que tenha um perfil de codificação de apagamento diferente. Se você precisar fazer essas alterações no ILM, você deve abortar o procedimento EC Rebalanceance.

Adicionar capacidade de metadados

Para garantir que o espaço adequado esteja disponível para metadados de objetos, talvez seja necessário executar um procedimento de expansão para adicionar novos nós de storage em cada local.

O StorageGRID reserva espaço para metadados de objetos no volume 0 de cada nó de storage. Três cópias de todos os metadados de objetos são mantidas em cada local, distribuídas uniformemente por todos os nós de storage.

Você pode usar o Grid Manager para monitorar a capacidade dos metadados dos nós de storage e estimar a rapidez com que a capacidade dos metadados está sendo consumida. Além disso, o alerta **armazenamento de metadados baixo** é acionado para um nó de armazenamento quando o espaço de metadados usado atinge determinados limites.

Observe que a capacidade de metadados de objetos de uma grade pode ser consumida mais rápido do que sua capacidade de armazenamento de objetos, dependendo de como você usa a grade. Por exemplo, se você costuma ingerir grandes quantidades de pequenos objetos ou adicionar grandes quantidades de metadados ou tags de usuários a objetos, talvez seja necessário adicionar nós de storage para aumentar a capacidade dos metadados, mesmo que haja capacidade suficiente de storage de objetos.

Para obter mais informações, consulte o seguinte:

- [Gerenciar o storage de metadados de objetos](#)
- [Monitore a capacidade dos metadados de objetos para cada nó de storage](#)

Diretrizes para aumentar a capacidade dos metadados

Antes de adicionar nós de storage para aumentar a capacidade dos metadados, leia as diretrizes e limitações a seguir:

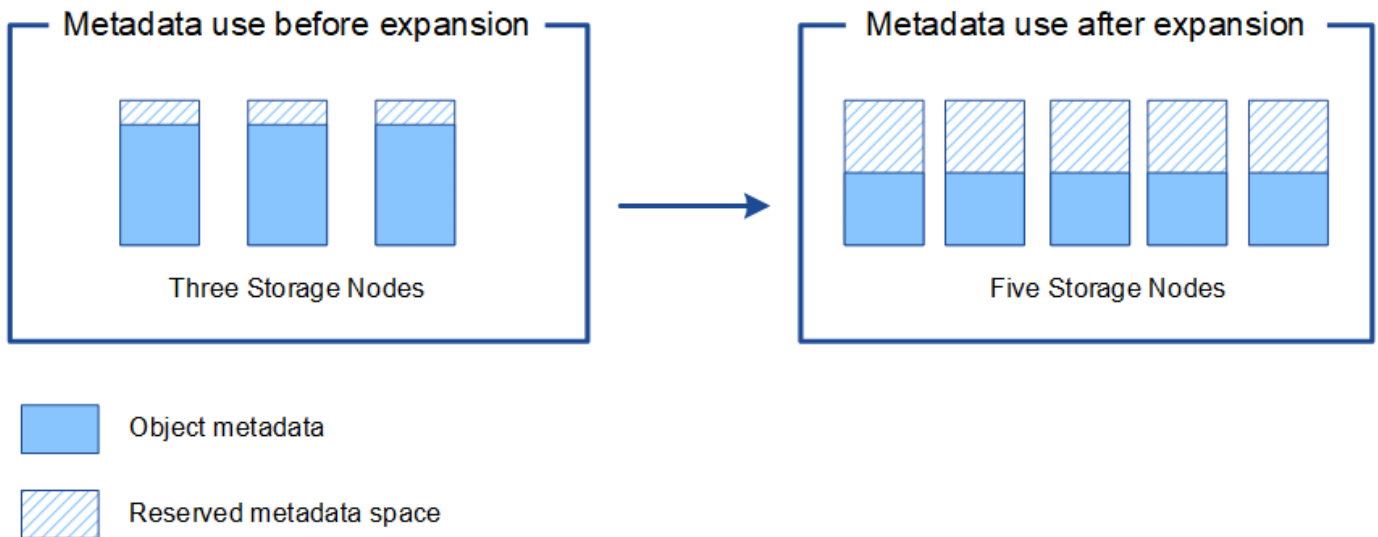
- Supondo que haja capacidade suficiente de storage de objetos disponível, ter mais espaço disponível para metadados de objetos aumenta o número de objetos que você pode armazenar no sistema StorageGRID.
- Você pode aumentar a capacidade de metadados de uma grade adicionando um ou mais nós de storage a cada local.
- O espaço real reservado para metadados de objetos em qualquer nó de armazenamento depende da opção de armazenamento de espaço reservado de metadados (configuração de todo o sistema), da quantidade de RAM alocada ao nó e do tamanho do volume do nó 0. Consulte as instruções para [Administrando o StorageGRID](#).
- Você não pode aumentar a capacidade dos metadados adicionando volumes de storage aos nós de storage existentes, porque os metadados são armazenados apenas no volume 0.
- Você não pode aumentar a capacidade dos metadados adicionando um novo local.
- O StorageGRID mantém três cópias de todos os metadados de objetos em todos os locais. Por esse motivo, a capacidade de metadados do sistema é limitada pela capacidade de metadados do seu menor local.
- Ao adicionar capacidade de metadados, você deve adicionar o mesmo número de nós de storage a cada local.

Como os metadados são redistribuídos quando você adiciona nós de storage

Quando você adiciona nós de storage a uma expansão, o StorageGRID redistribui os metadados de objetos existentes aos novos nós em cada local, o que aumenta a capacidade geral dos metadados da grade. Nenhuma ação do usuário é necessária.

A figura a seguir mostra como o StorageGRID redistribui os metadados de objetos quando você adiciona nós de storage em uma expansão. O lado esquerdo da figura representa o volume 0 de três nós de storage antes de uma expansão. Os metadados estão consumindo uma parte relativamente grande do espaço de metadados disponível de cada nó, e o alerta **armazenamento de metadados baixo** foi acionado.

O lado direito da figura mostra como os metadados existentes são redistribuídos depois que dois nós de storage são adicionados ao local. A quantidade de metadados em cada nó diminuiu, o alerta **armazenamento de metadados baixo** não é mais acionado e o espaço disponível para metadados aumentou.



Adicione nós de grade para adicionar recursos ao seu sistema

Você pode adicionar redundância ou recursos adicionais a um sistema StorageGRID adicionando novos nós de grade a sites existentes.

Por exemplo, você pode optar por adicionar nós de Gateway adicionais para suportar a criação de grupos de alta disponibilidade de nós de Gateway, ou você pode adicionar um nó de administrador em um site remoto para permitir o monitoramento usando um nó local.

Você pode adicionar um ou mais dos seguintes tipos de nós a um ou mais locais existentes em uma única operação de expansão:

- Nós de administração não primários
- Nós de storage
- Nós de gateway
- Nós de arquivamento

Ao se preparar para adicionar nós de grade, esteja ciente das seguintes limitações:

- O nó de administração principal é implantado durante a instalação inicial. Não é possível adicionar um nó de administração principal durante uma expansão.
- Você pode adicionar nós de storage e outros tipos de nós na mesma expansão.
- Ao adicionar nós de storage, você deve Planejar cuidadosamente o número e o local dos novos nós. [Diretrizes para adicionar capacidade de objeto](#) Consulte .
- Se você estiver adicionando nós de Arquivo, observe que cada nó de Arquivo só suporta fita por meio do middleware Tivoli Storage Manager (TSM).
- Se a opção **New Node Client Network Default** estiver definida como **unTrusted** na página redes de clientes não confiáveis, os aplicativos clientes que se conectam a nós de expansão usando a rede de cliente devem se conectar usando uma porta de endpoint do balanceador de carga (**CONFIGURATION > Network > UnTrusted Client Networks**). Consulte as instruções para [Administrando o StorageGRID](#) alterar a configuração do novo nó e configurar pontos de extremidade do balanceador de carga.

Adicione um novo site

Você pode expandir seu sistema StorageGRID adicionando um novo site.

Diretrizes para adicionar um site

Antes de adicionar um site, revise os seguintes requisitos e limitações:

- Só é possível adicionar um local por operação de expansão.
- Não é possível adicionar nós de grade a um site existente como parte da mesma expansão.
- Todos os locais devem incluir pelo menos três nós de storage.
- Adicionar um novo site não aumenta automaticamente o número de objetos que você pode armazenar. A capacidade total de objeto de uma grade depende da quantidade de storage disponível, da política de ILM e da capacidade de metadados em cada local.
- Ao dimensionar um novo local, você deve garantir que ele inclua capacidade suficiente de metadados.

O StorageGRID mantém uma cópia de todos os metadados de objetos em cada local. Ao adicionar um novo local, você deve garantir que ele inclua capacidade de metadados suficiente para os metadados de objetos existentes e capacidade de metadados suficiente para crescimento.

Para obter mais informações, consulte o seguinte:

- [Gerenciar o storage de metadados de objetos](#)
- [Monitore a capacidade dos metadados de objetos para cada nó de storage](#)
- Você deve considerar a largura de banda de rede disponível entre sites e o nível de latência de rede. As atualizações de metadados são continuamente replicadas entre sites, mesmo que todos os objetos sejam armazenados apenas no local onde são ingeridos.
- Como o sistema StorageGRID permanece operacional durante a expansão, você deve revisar as regras do ILM antes de iniciar o procedimento de expansão. Você deve garantir que as cópias de objeto não sejam armazenadas no novo local até que o procedimento de expansão seja concluído.

Por exemplo, antes de iniciar a expansão, determine se alguma regra usa o pool de storage padrão (todos os nós de storage). Se isso acontecer, você deverá criar um novo pool de storage que contenha os nós de storage existentes e atualizar suas regras de ILM para usar o novo pool de storage. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó nesse site se tornar ativo.

Para obter mais informações sobre como alterar o ILM ao adicionar um novo site, consulte o exemplo de alteração de uma política ILM nas instruções para [Gerenciando objetos com ILM](#).

Reúna os materiais necessários

Antes de executar uma operação de expansão, reúna os materiais e instale e configure qualquer novo hardware e redes.

Item	Notas
Arquivo de instalação do StorageGRID	<p>Se você estiver adicionando novos nós de grade ou um novo local, baixe e extraia o arquivo de instalação do StorageGRID. Você deve usar a mesma versão que está atualmente em execução na grade.</p> <p>Para obter detalhes, consulte as instruções para Transferir e extrair os ficheiros de instalação do StorageGRID.</p> <p>Observação: você não precisará baixar arquivos se estiver adicionando novos volumes de storage aos nós de storage existentes ou instalando um novo dispositivo StorageGRID.</p>
Serviço de laptop	<p>O computador portátil de serviço tem o seguinte:</p> <ul style="list-style-type: none"> • Porta de rede • Cliente SSH (por exemplo, PuTTY) • Navegador da Web suportado
Passwords.txt ficheiro	<p>Contém as senhas necessárias para acessar os nós de grade na linha de comando. Incluído no Pacote de recuperação.</p>
Frase-passe do provisionamento	<p>A frase-passe é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no Passwords.txt arquivo.</p>
Documentação do StorageGRID	<ul style="list-style-type: none"> • Administrar o StorageGRID • Notas de lançamento • Instruções de instalação para a sua plataforma <ul style="list-style-type: none"> ◦ Instale o Red Hat Enterprise Linux ou CentOS ◦ Instale Ubuntu ou Debian ◦ Instale o VMware
Documentação atual para a sua plataforma	<p>Para versões suportadas, consulte "Matriz de interoperabilidade".</p>

Baixe e extraia os arquivos de instalação do StorageGRID

Antes de poder adicionar novos nós de grade ou um novo site, você deve baixar o arquivo de instalação apropriado do StorageGRID e extrair os arquivos.

Sobre esta tarefa

Você deve executar operações de expansão usando a versão do StorageGRID que está atualmente em execução na grade.

Passos

1. Vá para a página de downloads do NetApp para StorageGRID.

["NetApp Downloads: StorageGRID"](#)

2. Selecione a versão do StorageGRID que está atualmente em execução na grade.
3. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.
4. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
5. Na coluna **Instalar StorageGRID** da página de download, selecione o `.tgz` arquivo ou `.zip` para sua plataforma.

A versão apresentada no ficheiro de arquivo de instalação tem de corresponder à versão do software atualmente instalado.

Use o `.zip` arquivo se você estiver executando o Windows no laptop de serviço.

Plataforma	Arquivo de instalação
Red Hat Enterprise Linux ou CentOS	<code>StorageGRID-Webscale-version-RPM-uniqueID.zip</code> <code>StorageGRID-Webscale-version-RPM-uniqueID.tgz</code>
Ubuntu ou Debian ou appliances	<code>StorageGRID-Webscale-version-DEB-uniqueID.zip</code> <code>StorageGRID-Webscale-version-DEB-uniqueID.tgz</code>
VMware	<code>StorageGRID-Webscale-version-VMware-uniqueID.zip</code> <code>StorageGRID-Webscale-version-VMware-uniqueID.tgz</code>
OpenStack/outro hipervisor	Para expandir uma implantação existente no OpenStack, você deve implantar uma máquina virtual executando uma das distribuições Linux suportadas listadas acima e seguir as instruções apropriadas para Linux.

6. Transfira e extraia o ficheiro de arquivo.
7. Siga a etapa apropriada para sua plataforma escolher os arquivos de que você precisa, com base em sua plataforma, topologia de grade planejada e como você expandirá seu sistema StorageGRID.

Os caminhos listados na etapa para cada plataforma são relativos ao diretório de nível superior instalado pelo arquivo de arquivo.

8. Se estiver expandindo um sistema Red Hat Enterprise Linux ou CentOS, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.

Caminho e nome do arquivo	Descrição
	Pacote RPM para instalar as imagens do nó StorageGRID em seus hosts RHEL ou CentOS.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL ou CentOS.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Exemplo de função do Ansible e manual de estratégia para configurar hosts RHEL ou CentOS para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Esquemas de API para StorageGRID. Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.

1. Se você estiver expandindo um sistema Ubuntu ou Debian, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.

Caminho e nome do arquivo	Descrição
	Um arquivo de licença do NetApp que não é de produção que pode ser usado para testes e implantações de prova de conceito.
	Pacote DEB para instalar as imagens do nó StorageGRID em hosts Ubuntu ou Debian.
	MD5 checksum para o arquivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Pacote DEB para instalar o serviço host StorageGRID em hosts Ubuntu ou Debian.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Exemplo Ansible role e playbook para configurar hosts Ubuntu ou Debian para a implantação de contentores StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	<p>Esquemas de API para StorageGRID.</p> <p>Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.</p>

1. Se você estiver expandindo um sistema VMware, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como um modelo para criar máquinas virtuais de nó de grade.
	O arquivo de modelo Open Virtualization Format (.ovf) e o arquivo de manifesto (.mf) para implantar o nó de administração principal.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de administração não primários.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de arquivamento.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós do Gateway.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de storage baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um exemplo de arquivo de configuração para uso com o <code>deploy-vsphere-ovftool.sh</code> script.
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.

Caminho e nome do arquivo	Descrição
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Esquemas de API para StorageGRID. Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.

1. Se você estiver expandindo um sistema baseado no StorageGRID Appliance, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	DEB pacote para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação do pacote de instalação DEB usado pelo instalador do dispositivo StorageGRID para validar se o pacote está intacto após o upload.



Para a instalação do dispositivo, esses arquivos só são necessários se você precisar evitar o tráfego de rede. O dispositivo pode baixar os arquivos necessários do nó de administração principal.

Verifique o hardware e a rede

Antes de iniciar a expansão do sistema StorageGRID, verifique o seguinte:

- O hardware necessário para suportar os novos nós de grade ou o novo site foi instalado e configurado.
- Todos os novos nós têm caminhos de comunicação bidirecionais para todos os nós existentes e novos (um requisito para a rede de Grade).
- O nó de administração principal pode se comunicar com todos os servidores de expansão destinados a hospedar o sistema StorageGRID.
- Se algum dos novos nós tiver um endereço IP de rede de Grade em uma sub-rede não usada anteriormente, você já [adicionada a nova sub-rede](#) terá acesso à lista de sub-redes de rede de Grade.

Caso contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar o procedimento novamente.

- Você não está usando a tradução de endereço de rede (NAT) na rede de Grade entre nós de grade ou entre sites do StorageGRID. Quando você usa endereços IPv4 privados para a rede de Grade, esses endereços devem ser roteáveis diretamente de cada nó de grade em cada local. O uso de NAT para fazer a ponte da rede de Grade em um segmento de rede pública é suportado somente se você usar um aplicativo de encapsulamento transparente para todos os nós da grade, o que significa que os nós da grade não exigem conhecimento de endereços IP públicos.

Esta restrição NAT é específica para nós de grade e rede de grade. Conforme necessário, você pode usar o NAT entre clientes externos e nós de grade, por exemplo, para fornecer um endereço IP público para um nó de gateway.

Adicione volumes de armazenamento

Adicionar volumes de storage aos nós de storage

Você pode expandir a capacidade de storage dos nós de storage que têm 16 ou menos volumes de storage adicionando volumes de storage adicionais. Talvez você precise adicionar volumes de storage a mais de um nó de storage para atender aos requisitos de ILM para cópias replicadas ou codificadas por apagamento.

O que você vai precisar

Antes de adicionar volumes de armazenamento, consulte o [diretrizes para adicionar capacidade de objeto](#) para garantir que você saiba onde adicionar volumes para atender aos requisitos da política de ILM.



Estas instruções se aplicam somente a nós de storage baseados em software. [Adicione o compartimento de expansão ao SG6060 ou SG6060X implantados](#) Consulte para saber como adicionar volumes de armazenamento ao SG6060 ou SG6060X instalando os compartimentos de expansão. Não é possível expandir os nós de storage de outros dispositivos.

Sobre esta tarefa

O storage subjacente de um nó de storage é dividido em vários volumes de storage. Os volumes de armazenamento são dispositivos de armazenamento baseados em blocos que são formatados pelo sistema StorageGRID e montados para armazenar objetos. Cada nó de armazenamento pode suportar até 16 volumes de armazenamento, que são chamados *armazenamentos de objetos* no Gerenciador de Grade.



Os metadados de objetos são sempre armazenados no armazenamento de objetos 0.

Cada armazenamento de objetos é montado em um volume que corresponde ao seu ID. Por exemplo, o armazenamento de objetos com uma ID de 0000 corresponde ao `/var/local/rangedb/0` ponto de montagem.

Antes de adicionar novos volumes de armazenamento, use o Gerenciador de Grade para exibir os armazenamentos de objetos atuais para cada nó de armazenamento, bem como os pontos de montagem correspondentes. Você pode usar essas informações ao adicionar volumes de armazenamento.

Passos

1. Selecione **NÓS** > **site** > **Storage Node** > **Storage**.
2. Role para baixo para ver as quantidades de armazenamento disponível para cada volume e

armazenamento de objetos.

Para nós de storage de dispositivo, o Nome Mundial para cada disco corresponde ao identificador mundial de volume (WWID) que aparece quando você visualiza as propriedades de volume padrão no software SANtricity (o software de gerenciamento conectado ao controlador de storage 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
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

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

Object stores

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

3. Siga as instruções da sua plataforma para adicionar novos volumes de armazenamento ao nó de armazenamento.
 - [VMware: Adicione volumes de storage ao nó de storage](#)
 - [Linux: Adicione volumes de SAN ou de conexão direta ao nó de storage](#)

VMware: Adicione volumes de storage ao nó de storage

Se um nó de storage incluir menos de 16 volumes de storage, você poderá aumentar sua capacidade usando o VMware vSphere para adicionar volumes.

O que você vai precisar

- Você tem acesso às instruções para instalar implantações do StorageGRID para VMware.
 - [Instale o VMware](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem permissões de acesso específicas.



Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento não está disponível por um breve período de tempo quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de storage de cada vez para evitar afetar os serviços de grade voltados para o cliente.

Passos

1. Se necessário, instale um novo hardware de armazenamento e crie novos armazenamentos de dados VMware.
2. Adicione um ou mais discos rígidos à máquina virtual para uso como armazenamento (armazenamentos de objetos).
 - a. Abra o VMware vSphere Client.
 - b. Edite as configurações da máquina virtual para adicionar um ou mais discos rígidos adicionais.

Os discos rígidos são normalmente configurados como discos de máquina virtual (VMDKs). Os VMDKs são mais comumente usados e são mais fáceis de gerenciar, enquanto os RDMs podem fornecer melhor desempenho para cargas de trabalho que usam tamanhos de objetos maiores (por exemplo, maiores que 100 MB). Para obter mais informações sobre como adicionar discos rígidos a máquinas virtuais, consulte a documentação do VMware vSphere.

3. Reinicie a máquina virtual usando a opção **Restart Guest os** no VMware vSphere Client ou inserindo o seguinte comando em uma sessão ssh na máquina virtual:`sudo reboot`



Não use **Desligar** ou **Redefinir** para reiniciar a máquina virtual.

4. Configure o novo armazenamento para uso pelo nó de armazenamento:
 - a. Faça login no nó da grade:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

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

b. Configure os novos volumes de armazenamento:

```
sudo add_rangedbs.rb
```

Este script encontra quaisquer novos volumes de armazenamento e solicita que você os formate.

- a. Digite **y** para aceitar a formatação.
- b. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.
 - Introduza **y** para reformatar.
 - Digite **n** para ignorar a reformatação.
- c. Quando solicitado, digite **y** para interromper os serviços de armazenamento.

Os serviços de armazenamento são interrompidos e o `setup_rangedbs.sh` script é executado automaticamente. Depois que os volumes estiverem prontos para uso como `rangedbs`, os serviços começam novamente.

5. Verifique se os serviços começam corretamente:

- a. Exibir uma lista do status de todos os serviços no servidor:

```
sudo storagegrid-status
```

O estado é atualizado automaticamente.

- a. Aguarde até que todos os serviços estejam em execução ou verificados.
- b. Saia do ecrã de estado:

```
Ctrl+C
```

6. Verifique se o nó de storage está on-line:

- a. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
- b. Selecione **SUPPORT > Tools > Grid topology**.
- c. Selecione **site > Storage Node > LDR > Storage**.
- d. Selecione a guia **Configuração** e a guia **Principal**.
- e. Se a lista suspensa **Estado de armazenamento - desejado** estiver definida como somente leitura ou Offline, selecione **Online**.
- f. Selecione **aplicar alterações**.

7. Para ver os novos armazenamentos de objetos:

- a. Selecione **NÓS > site > Storage Node > Storage**.
- b. Veja os detalhes na tabela **Object Stores**.

Resultado

Você pode usar a capacidade expandida dos nós de storage para salvar dados de objetos.

Linux: Adicione volumes de SAN ou de conexão direta ao nó de storage

Se um nó de armazenamento incluir menos de 16 volumes de armazenamento, você poderá aumentar sua capacidade adicionando novos dispositivos de armazenamento de bloco, tornando-os visíveis aos hosts Linux e adicionando os novos mapeamentos de dispositivo de bloco ao arquivo de configuração do StorageGRID usado para o nó de armazenamento.

O que você vai precisar

- Você tem acesso às instruções para instalar o StorageGRID para sua plataforma Linux.
 - [Instale o Red Hat Enterprise Linux ou CentOS](#)
 - [Instale Ubuntu ou Debian](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem permissões de acesso específicas.



Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento não está disponível por um breve período de tempo quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de storage de cada vez para evitar afetar os serviços de grade voltados para o cliente.

Passos

1. Instale o novo hardware de armazenamento.

Para obter mais informações, consulte a documentação fornecida pelo fornecedor de hardware.

2. Crie novos volumes de armazenamento de blocos dos tamanhos desejados.
 - Anexe as novas unidades de disco e atualize a configuração do controlador RAID conforme necessário, ou aloque os novos LUNs SAN nos storages de armazenamento compartilhados e permita que o host Linux os acesse.
 - Use o mesmo esquema de nomenclatura persistente usado para os volumes de storage no nó de storage existente.
 - Se você usar o recurso de migração de nó do StorageGRID, torne os novos volumes visíveis para outros hosts Linux que são destinos de migração para este nó de storage. Para obter mais informações, consulte as instruções para instalar o StorageGRID para sua plataforma Linux.
3. Faça login no host Linux que suporta o nó de storage como raiz ou com uma conta que tenha permissão `sudo`.
4. Confirme se os novos volumes de armazenamento estão visíveis no host Linux.

Talvez seja necessário voltar a digitalizar dispositivos.

5. Execute o seguinte comando para desativar temporariamente o nó de armazenamento:

```
sudo storagegrid node stop <node-name>
```

6. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó para o nó de armazenamento, que pode ser encontrado em `/etc/storagegrid/nodes/<node-name>.conf`.
7. Localize a seção do arquivo de configuração do nó que contém os mapeamentos de dispositivo de bloco de armazenamento de objetos existentes.

No exemplo, `BLOCK_DEVICE_RANGEDB_00` `BLOCK_DEVICE_RANGEDB_03` para são os mapeamentos de dispositivo de bloco de armazenamento de objetos existentes.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Adicione novos mapeamentos de dispositivo de bloco de armazenamento de objetos correspondentes aos volumes de armazenamento de bloco adicionados para este nó de armazenamento.

Certifique-se de começar no `BLOCK_DEVICE_RANGEDB_nn` próximo . Não deixe uma folga.

- Com base no exemplo acima, comece em `BLOCK_DEVICE_RANGEDB_04`.
- No exemplo abaixo, quatro novos volumes de armazenamento de bloco foram adicionados ao nó:
`BLOCK_DEVICE_RANGEDB_04` Para `BLOCK_DEVICE_RANGEDB_07`.

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

9. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó para o nó de armazenamento:

```
sudo storagegrid node validate <node-name>
```

Solucione quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

Se você observar um erro semelhante ao seguinte, isso significa que o arquivo de configuração do nó está tentando mapear o dispositivo de bloco usado por <node-name> para para para <PURPOSE> dado <path-name> no sistema de arquivos Linux, mas não há um arquivo especial válido de dispositivo de bloco (ou softlink para um arquivo especial de dispositivo de bloco) nesse local.



```

Checking configuration file for node <node-name>...
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device

```

Verifique se você inseriu o <path-name> correto .

10. Execute o seguinte comando para reiniciar o nó com os novos mapeamentos de dispositivo de bloco em vigor:

```
sudo storagegrid node start <node-name>
```

11. Faça login no nó de armazenamento como administrador usando a senha listada no `Passwords.txt` arquivo.

12. Verifique se os serviços começam corretamente:

- a. Veja uma lista do status de todos os serviços no servidor `sudo storagegrid-status`

O estado é atualizado automaticamente.

- b. Aguarde até que todos os serviços estejam em execução ou verificados.
- c. Saia do ecrã de estado:

```
Ctrl+C
```

13. Configure o novo armazenamento para uso pelo nó de armazenamento:

- a. Configure os novos volumes de armazenamento:

```
sudo add_rangedbs.rb
```

Este script encontra quaisquer novos volumes de armazenamento e solicita que você os formate.

- a. Digite **y** para formatar os volumes de armazenamento.
- b. Se algum dos volumes tiver sido formatado anteriormente, decida se deseja reformatá-los.
 - Introduza **y** para reformatar.
 - Digite **n** para ignorar a reformatação.
- c. Quando solicitado, digite **y** para interromper os serviços de armazenamento.

Os serviços de armazenamento são interrompidos e o `setup_rangedbs.sh` script é executado automaticamente. Depois que os volumes estiverem prontos para uso como `rangedbs`, os serviços começam novamente.

14. Verifique se os serviços começam corretamente:

- a. Exibir uma lista do status de todos os serviços no servidor:

```
sudo storagegrid-status
```

O estado é atualizado automaticamente.

- a. Aguarde até que todos os serviços estejam em execução ou verificados.
- b. Saia do ecrã de estado:

```
Ctrl+C
```

15. Verifique se o nó de storage está on-line:

- a. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
- b. Selecione **SUPPORT > Tools > Grid topology**.
- c. Selecione **site > Storage Node > LDR > Storage**.
- d. Selecione a guia **Configuração** e a guia **Principal**.
- e. Se a lista suspensa **Estado de armazenamento - desejado** estiver definida como somente leitura ou Offline, selecione **Online**.
- f. Clique em **aplicar alterações**.

16. Para ver os novos armazenamentos de objetos:

- a. Selecione **NÓS > site > Storage Node > Storage**.

b. Veja os detalhes na tabela **Object Stores**.

Resultado

Agora você pode usar a capacidade expandida dos nós de storage para salvar dados de objetos.

Adicione nós de grade ou local

Adicione nós de grade ao site existente ou adicione um novo site

Você pode seguir este procedimento para adicionar nós de grade a sites existentes ou adicionar um novo site, mas não pode executar ambos os tipos de expansão ao mesmo tempo.

O que você vai precisar

- Você tem a permissão de Acesso root ou Manutenção.
- Todos os nós existentes na grade estão ativos e em execução em todos os locais.
- Todos os procedimentos anteriores de expansão, atualização, desativação ou recuperação estão concluídos.



Você é impedido de iniciar uma expansão enquanto outro procedimento de expansão, atualização, recuperação ou desativação ativa está em andamento. No entanto, se necessário, você pode pausar um procedimento de desativação para iniciar uma expansão.

Passos

1. [Atualizar sub-redes para rede de Grade.](#)
2. [Implantar novos nós de grade.](#)
3. [Execute a expansão.](#)

Atualizar sub-redes para rede de Grade

Quando você adiciona nós de grade ou um novo site em uma expansão, talvez seja necessário atualizar ou adicionar sub-redes à rede de Grade.

O StorageGRID mantém uma lista das sub-redes de rede usadas para se comunicar entre nós de grade na rede de grade (eth0). Essas entradas incluem as sub-redes usadas para a rede de Grade por cada site em seu sistema StorageGRID, bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway rede de Grade.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento.
- Você tem os endereços de rede, na notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se algum dos novos nós tiver um endereço IP de rede de Grade em uma sub-rede não usada anteriormente, você deve adicionar a nova sub-rede à lista de sub-rede de Grade antes de iniciar a expansão. Caso contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar o procedimento novamente.

Passos

1. Selecione **MAINTENANCE > Network > Grid Network**.

Grid Network

Configure the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network (eth0) for each site in your StorageGRID system as well as any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnets

Subnet 1



Passphrase

Provisioning
Passphrase

Save

2. Na lista sub-redes, selecione o sinal de mais para adicionar uma nova sub-rede na notação CIDR.
Por exemplo, digite 10.96.104.0/22.
3. Insira a senha de provisionamento e selecione **Salvar**.

As sub-redes especificadas são configuradas automaticamente para o sistema StorageGRID.

Implantar novos nós de grade

As etapas para implantar novos nós de grade em uma expansão são as mesmas que as etapas usadas quando a grade foi instalada pela primeira vez. Você deve implantar todos os novos nós de grade antes de executar a expansão.

Quando você expande a grade, os nós adicionados não precisam corresponder aos tipos de nó existentes. Você pode adicionar nós VMware, nós baseados em contêiner do Linux ou nós de dispositivo.

VMware: Implante nós de grade

É necessário implantar uma máquina virtual no VMware vSphere para cada nó VMware que você deseja adicionar à expansão.

Passos

1. [Implante o novo nó como máquina virtual](#) E conecte-o a uma ou mais redes StorageGRID.

Ao implantar o nó, você pode opcionalmente remapear as portas dos nós ou aumentar as configurações de CPU ou memória.

2. Depois de implantar todos os novos nós da VMware, [execute o procedimento de expansão](#).

Linux: Implante nós de grade

Você pode implantar nós de grade em novos hosts Linux ou em hosts Linux existentes. Se você precisar de hosts Linux adicionais para dar suporte aos requisitos de CPU, RAM e storage dos nós StorageGRID que deseja adicionar à sua grade, você os prepara da mesma maneira que preparou os hosts quando os instalou pela primeira vez. Em seguida, você implanta os nós de expansão da mesma maneira que implantou nós de grade durante a instalação.

O que você vai precisar

- Você tem as instruções para instalar o StorageGRID para sua versão do Linux e analisou os requisitos de hardware e armazenamento.
 - [Instale o Red Hat Enterprise Linux ou CentOS](#)
 - [Instale Ubuntu ou Debian](#)
- Se você planeja implantar novos nós de grade em hosts existentes, confirmou que os hosts existentes têm capacidade suficiente de CPU, RAM e storage para os nós adicionais.
- Você tem um plano para minimizar domínios de falha. Por exemplo, você não deve implantar todos os nós do Gateway em um único host físico.



Em uma implantação de produção, não execute mais de um nó de storage em um único host físico ou virtual. O uso de um host dedicado para cada nó de storage fornece um domínio de falha isolado.

- Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp ONTAP, confirme se o volume não tem uma política de disposição em camadas do FabricPool habilitada. A desativação da disposição em camadas do FabricPool para volumes usados com nós do StorageGRID simplifica a solução de problemas e as operações de storage.

Passos

1. Se você estiver adicionando novos hosts, acesse as instruções de instalação para implantar nós do StorageGRID.
2. Para implantar os novos hosts, siga as instruções para preparar os hosts.
3. Para criar arquivos de configuração de nós e validar a configuração do StorageGRID, siga as instruções para implantar nós de grade.
4. Se você estiver adicionando nós a um novo host Linux, inicie o serviço de host StorageGRID.
5. Se você estiver adicionando nós a um host Linux existente, inicie os novos nós usando a CLI do serviço de host do StorageGRID:

```
sudo storagegrid node start [<node name>]
```

Depois de terminar

Depois de implantar todos os novos nós de grade, você pode [execute a expansão](#).

Dispositivos: Implantando nós de administração não primários, de gateway ou storage de storage

Para instalar o software StorageGRID em um nó de dispositivo, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo. Em uma expansão, cada dispositivo de storage funciona como um nó de storage único e cada dispositivo de serviços funciona como um nó de gateway único ou nó de administração não primário. Qualquer dispositivo pode se conectar à rede de Grade, à rede Admin e à rede Cliente.

O que você vai precisar

- O dispositivo foi instalado em um rack ou gabinete, conectado às redes e ligado.

- Você usou o Instalador de dispositivos StorageGRID para concluir todas as etapas "configurar hardware" nas instruções de instalação e manutenção do dispositivo.
 - [Aparelhos de serviços SG100 e SG1000](#)
 - [Configurar hardware \(SG5600\)](#)
 - [Configurar hardware \(SG5700\)](#)
 - [Configurar hardware \(SG6000\)](#)

A configuração do hardware do dispositivo inclui as etapas necessárias para configurar conexões StorageGRID (links de rede e endereços IP), bem como as etapas opcionais para habilitar a criptografia de nós, alterar o modo RAID e remapeamento de portas de rede.

- Todas as sub-redes de rede listadas na página Configuração IP do Instalador de dispositivos StorageGRID foram definidas na Lista de sub-redes de rede de Grade no nó de administração principal.
- O firmware do instalador do dispositivo StorageGRID no dispositivo de substituição é compatível com a versão do software StorageGRID atualmente em execução na grelha. Por exemplo, a versão 3,6 do Instalador de dispositivos StorageGRID é compatível com a versão 11,6 do StorageGRID. (Se as versões não forem compatíveis, você deve atualizar o firmware do instalador do dispositivo StorageGRID.)
- Você tem um laptop de serviço com um [navegador da web suportado](#).
- Você conhece um dos endereços IP atribuídos ao controlador de computação do dispositivo. Você pode usar o endereço IP de qualquer rede StorageGRID conectada.

Sobre esta tarefa

O processo de instalação do StorageGRID em um nó de dispositivo tem as seguintes fases:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó do dispositivo.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.

Ao longo das tarefas de instalação do dispositivo, a instalação é interrompida. Para retomar a instalação, faça login no Gerenciador de Grade, aprove todos os nós de grade e conclua o processo de instalação do StorageGRID.



Se você precisar implantar vários nós de dispositivo de uma só vez, você pode automatizar o processo de instalação usando o `configure-sga.py` script de instalação do appliance.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo.

```
https://Controller_IP:8443
```

A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Na seção **nó de administração principal**, determine se você precisa especificar o endereço IP do nó de administração principal.

Se você já instalou outros nós nesse data center, o Instalador do StorageGRID Appliance poderá descobrir esse endereço IP automaticamente, assumindo que o nó de administrador principal ou pelo menos um outro nó de grade com ADMIN_IP configurado, está presente na mesma sub-rede.

3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Descrição
Entrada de IP manual	<ol style="list-style-type: none"> Desmarque a caixa de seleção Ativar descoberta de nó de administrador. Introduza o endereço IP manualmente. Clique em Salvar. Aguarde até que o estado da ligação para que o novo endereço IP fique pronto.
Detecção automática de todos os nós de administração principal conectados	<ol style="list-style-type: none"> Marque a caixa de seleção Enable Admin Node Discovery (Ativar descoberta de nó de administrador). Aguarde até que a lista de endereços IP descobertos seja exibida. Selecione o nó de administração principal para a grade onde este nó de storage do dispositivo será implantado. Clique em Salvar. Aguarde até que o estado da ligação para que o novo endereço IP fique pronto.

- No campo **Nome do nó**, insira o nome que deseja usar para este nó de appliance e selecione **Salvar**.

O nome do nó é atribuído a este nó do dispositivo no sistema StorageGRID. Ele é mostrado na página de nós (guia Visão geral) no Gerenciador de Grade. Se necessário, você pode alterar o nome ao aprovar o nó.

- Na seção **Instalação**, confirme se o estado atual é "Pronto para iniciar a instalação de *node name* na grade com Admin Node primário *admin_ip*" e que o botão **Start Installation** está ativado.

Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

- Na página inicial do Instalador de dispositivos StorageGRID, selecione **Iniciar instalação**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.

7. Se a expansão incluir vários nós de dispositivo, repita as etapas anteriores para cada dispositivo.



Se você precisar implantar vários nós de storage de dispositivos de uma só vez, poderá automatizar o processo de instalação usando o script de instalação do dispositivo configure-sga.py.

8. Se precisar acessar manualmente a página Instalação do Monitor, selecione **Instalação do Monitor** na barra de menus.

A página Instalação do monitor mostra o progresso da instalação.

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete	
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete	
Configure volumes	<div style="width: 30%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-00	
Configure host settings	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending	
2. Install OS			Pending
3. Install StorageGRID			Pending
4. Finalize installation			Pending

A barra de status azul indica qual tarefa está atualmente em andamento. As barras de estado verdes indicam tarefas concluídas com êxito.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver reexecutando uma instalação, todas as tarefas que não precisam ser executadas novamente serão mostradas com uma barra de status verde e um status de "pulado".

9. Reveja o progresso das duas primeiras fases de instalação.

1. Configure o appliance

Durante esta fase, ocorre um dos seguintes processos:

- Para um dispositivo de armazenamento, o instalador se conecta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.
- Para um dispositivo de serviços, o instalador limpa qualquer configuração existente das unidades no controlador de computação e configura as configurações do host.

2. Instale o os

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

10. Continue monitorando o progresso da instalação até que uma mensagem seja exibida na janela do console, solicitando que você use o Gerenciador de Grade para aprovar o nó.



Aguarde até que todos os nós adicionados nessa expansão estejam prontos para aprovação antes de ir para o Gerenciador de Grade para aprovar os nós.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Execute a expansão

Quando você executa a expansão, os novos nós de grade são adicionados à implantação existente do StorageGRID.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento.
- Você implantou todos os nós de grade que estão sendo adicionados a essa expansão.

- Se você estiver adicionando nós de storage, confirmará que todas as operações de reparo de dados executadas como parte de uma recuperação estão concluídas. [Verifique os trabalhos de reparação de dados](#)Consulte .
- Se você estiver adicionando um novo site, deverá revisar e atualizar as regras do ILM antes de iniciar o procedimento de expansão para garantir que as cópias de objeto não sejam armazenadas no novo site até que a expansão seja concluída. Por exemplo, se uma regra usar o pool de storage padrão (todos os nós de storage), será necessário criar um novo pool de storage que contenha apenas os nós de storage existentes e atualizar a regra ILM para usar o novo pool de storage. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó nesse site se tornar ativo. Consulte as instruções para [Gerenciando objetos com ILM](#).

Sobre esta tarefa

A execução da expansão inclui estas fases:

1. Configure a expansão especificando se você está adicionando novos nós de grade ou um novo site e aprovando os nós de grade que deseja adicionar.
2. Você inicia a expansão.
3. Enquanto o processo de expansão estiver em execução, você baixa um novo arquivo do Pacote de recuperação.
4. Você monitora o status dos estágios de configuração da grade, que são executados automaticamente. O conjunto de estágios depende de quais tipos de nós de grade estão sendo adicionados e se um novo site está sendo adicionado.



Alguns estágios podem levar uma quantidade significativa de tempo para serem executados em uma grade grande. Por exemplo, o streaming do Cassandra para um novo nó de armazenamento pode levar apenas alguns minutos se o banco de dados do Cassandra estiver vazio. No entanto, se o banco de dados Cassandra incluir uma grande quantidade de metadados de objetos, essa etapa pode levar várias horas ou mais. Não reinicie nenhum nó de armazenamento durante os estágios "expandindo o cluster Cassandra" ou "iniciando Cassandra e streaming de dados".

Passos

1. Selecione **MAINTENANCE > Tasks > Expansion**.

A página expansão da grade é exibida. A seção Pending Nodes lista todos os nós que estão prontos para serem adicionados.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

[Configure Expansion](#)

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
<input type="radio"/>	00:50:56:87:68:1a	DC2-ADM1-184	Admin Node	VMware VM	172.17.3.184/21
<input type="radio"/>	00:50:56:87:f1:fc	DC2-S1-185	Storage Node	VMware VM	172.17.3.185/21
<input type="radio"/>	00:50:56:87:54:1e	DC2-S2-186	Storage Node	VMware VM	172.17.3.186/21
<input type="radio"/>	00:50:56:87:6f:0c	DC2-S3-187	Storage Node	VMware VM	172.17.3.187/21
<input type="radio"/>	00:50:56:87:b6:83	DC2-S4-188	Storage Node	VMware VM	172.17.3.188/21
<input type="radio"/>	00:50:56:87:b3:7d	DC2-ARC1-189	Archive Node	VMware VM	172.17.3.189/21

2. Selecione **Configurar expansão**.

A caixa de diálogo seleção de local é exibida.

Site Selection

You can add grid nodes to a new site or to existing sites, but you cannot perform both types of expansion at the same time.

Site New Existing

Site Name

3. Selecione o tipo de expansão que você está iniciando:

- Se você estiver adicionando um novo site, selecione **novo** e digite o nome do novo site.
- Se você estiver adicionando nós de grade a um site existente, selecione **existente**.

4. Selecione **Guardar**.

5. Revise a lista **Pending Nodes** e confirme que ela mostra todos os nós de grade implantados.

Conforme necessário, você pode passar o cursor sobre o **Grid Network MAC Address** de um nó para ver detalhes sobre esse nó.

+ Approve
* Remove

Grid Network MAC	
<input type="radio"/>	00:50:56:87:68:1a
<input type="radio"/>	00:50:56:87:54:1e
<input type="radio"/>	00:50:56:87:6f:0c
<input type="radio"/>	00:50:56:87:b6:83
<input type="radio"/>	00:50:56:87:b3:7d

DC2-S3-187

Storage Node

Address	Name
Network	
Grid Network	172.17.3.187/21 172.17.0.1
Admin Network	
Client Network	10.224.3.187/21 10.224.0.1

Hardware

VMware VM 8 CPUs 8 GB RAM

Disks

107 GB 107 GB 107 GB 107 GB 107 GB



Se um nó de grade estiver ausente, confirme que ele foi implantado com sucesso.

6. Na lista de nós pendentes, aprove os nós de grade para essa expansão.
 - a. Selecione o botão de opção ao lado do primeiro nó de grade pendente que você deseja aprovar.
 - b. Selecione **Approve**.

O formulário de configuração do nó de grade é exibido.

Storage Node Configuration

General Settings

Site	<input type="text" value="Site A"/>
Name	<input type="text" value="DC2-S3-187"/>
NTP Role	<input type="text" value="Automatic"/>
ADC Service	<input type="text" value="Automatic"/>

Select "Yes" if this node will replace another node at this site that has the ADC service.

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text" value="172.17.3.187/21"/>
Gateway	<input type="text" value="172.17.0.1"/>

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text"/>
Gateway	<input type="text"/>
Subnets (CIDR)	<input type="text"/> +

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	<input type="text"/>
Gateway	<input type="text"/>

Cancel

Save

c. Conforme necessário, modifique as definições gerais:

- **Site:** O nome do site ao qual o nó da grade será associado. Se você estiver adicionando vários nós, certifique-se de selecionar o local correto para cada nó. Se você estiver adicionando um novo site, todos os nós serão adicionados ao novo site.

- **Nome:** O nome do host que será atribuído ao nó e o nome que será exibido no Gerenciador de Grade.
- **Função NTP:** A função Network Time Protocol (NTP) do nó de grade. As opções são **Automático**, **primário** e **Cliente**. A seleção de **Automático** atribui a função primária a nós de administração, nós de armazenamento com serviços ADC, nós de gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós de grade recebem a função Cliente.



Atribua a função NTP primária a pelo menos dois nós em cada local. Isso fornece acesso redundante ao sistema a fontes de temporização externas.

- **ADC Service** (somente nós de armazenamento): Se este nó de armazenamento executará o serviço controlador de domínio administrativo (ADC). O serviço ADC mantém o controle da localização e disponibilidade dos serviços da grade. Pelo menos três nós de storage em cada local devem incluir o serviço ADC. Você não pode adicionar o serviço ADC a um nó depois que ele é implantado.
 - Se você estiver adicionando esse nó para substituir um nó de armazenamento, selecione **Sim** se o nó que você está substituindo incluir o serviço ADC. Como você não pode desativar um nó de armazenamento se houver poucos serviços ADC, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido.
 - Caso contrário, selecione **Automático** para permitir que o sistema determine se esse nó requer o serviço ADC. Saiba mais sobre o quórum de ADC [aqui](#).
- d. Conforme necessário, modifique as configurações para rede de Grade, rede de Admin e rede de cliente.
- **Endereço IPv4 (CIDR):** O endereço de rede CIDR para a interface de rede. Por exemplo: 172.16.10.100/24
 - **Gateway:** O gateway padrão do nó de grade. Por exemplo: 172.16.10.1
 - **Sub-redes (CIDR):** Uma ou mais sub-redes para a rede Admin.
- e. Selecione **Guardar**.

O nó de grade aprovado move-se para a lista de nós aprovados.

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
00:50:56:87:f1:fc	DC2-S1-185	Site A	Storage Node	VMware VM	172.17.3.185/21
00:50:56:87:6f:0c	DC2-S3-187	Site A	Storage Node	VMware VM	172.17.3.187/21

Passphrase

Enter the provisioning passphrase to change the grid topology of your StorageGRID system.

Provisioning Passphrase

- Para modificar as propriedades de um nó de grade aprovado, selecione seu botão de opção e selecione **Editar**.

- Para mover um nó de grade aprovado de volta para a lista de nós pendentes, selecione seu botão de opção e selecione **Reset**.
- Para remover permanentemente um nó de rede aprovado, desligue o nó. Em seguida, selecione o botão de opção e selecione **Remove**.

f. Repita estas etapas para cada nó de grade pendente que você deseja aprovar.



Se possível, você deve aprovar todas as notas de grade pendentes e executar uma única expansão. Mais tempo será necessário se você executar múltiplas expansões pequenas.

7. Quando tiver aprovado todos os nós de grade, digite a **frase-passe de provisionamento** e selecione **expandir**.

Após alguns minutos, esta página é atualizada para exibir o status do procedimento de expansão. Quando as tarefas que afetam o nó de grade individual estão em andamento, a seção Status do nó de grade lista o status atual de cada nó de grade.



Durante esse processo, para os aparelhos, o Instalador do StorageGRID Appliance mostra a instalação passando do Estágio 3 para o Estágio 4, finalize a Instalação. Quando a fase 4 é concluída, o controlador é reinicializado.

Grid Expansion

i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing Grid Nodes In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Q

Name	Site	Grid Network IPv4 Address	Progress	Stage
DC2-ADM1-184	Site A	172.17.3.184/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for NTP to synchronize
DC2-S1-185	Site A	172.17.3.185/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for Dynamic IP Service peers
DC2-S2-186	Site A	172.17.3.186/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for NTP to synchronize
DC2-S3-187	Site A	172.17.3.187/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for NTP to synchronize
DC2-S4-188	Site A	172.17.3.188/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for Dynamic IP Service peers
DC2-ARC1-189	Site A	172.17.3.189/21	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	Waiting for NTP to synchronize

2. Initial Configuration	Pending
3. Distributing the new grid node's certificates to the StorageGRID system.	Pending
4. Starting services on the new grid nodes	Pending
5. Cleaning up unused Cassandra keys	Pending



Uma expansão de site inclui uma tarefa adicional para configurar o Cassandra para o novo site.

8. Assim que o link **Download Recovery Package** for exibido, baixe o arquivo Recovery Package.

Você deve baixar uma cópia atualizada do arquivo do Pacote de recuperação o mais rápido possível após fazer alterações na topologia da grade no sistema StorageGRID. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

- a. Selecione a ligação de transferência.
- b. Digite a senha de provisionamento e selecione **Iniciar download**.
- c. Quando o download for concluído, abra o `.zip` arquivo e confirme que ele inclui um `gpt-backup` diretório e um `_SAID.zip` arquivo. Em seguida, extraia o `_SAID.zip` arquivo, vá para `/GID*_REV*` o diretório e confirme que você pode abrir o `passwords.txt` arquivo.
- d. Copie o arquivo do Pacote de recuperação baixado (`.zip`) para dois locais seguros, seguros e separados.



O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

9. Siga as instruções para adicionar um nó de armazenamento a um site existente ou adicionar um novo site.

Adicione nó de storage ao site existente

Se você estiver adicionando um ou mais nós de storage a um site existente, monitore o progresso da etapa "iniciando Cassandra e streaming de dados", revisando a porcentagem mostrada na mensagem de status.

4. Starting services on the new grid nodes In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Q

Name	Site	Grid Network IPv4 Address	Progress	Stage
DC1-S4	Data Center 1	10.96.99.55/23	<div style="width: 90%; height: 10px; background: linear-gradient(to right, #007bff, #007bff);"></div>	Starting Cassandra and streaming data (90.0% streamed)
DC1-S5	Data Center 1	10.96.99.56/23	<div style="width: 100%; height: 10px; background: #28a745;"></div>	Complete
DC1-S6	Data Center 1	10.96.99.57/23	<div style="width: 100%; height: 10px; background: #28a745;"></div>	Complete

Essa porcentagem estima o quão completa é a operação de streaming do Cassandra, com base na quantidade total de dados do Cassandra disponíveis e na quantidade que já foi gravada no novo nó.



Não reinicie nenhum nó de storage durante os estágios "expandindo o cluster Cassandra" ou "iniciando Cassandra e streaming de dados". Esses estágios podem levar muitas horas para serem concluídos para cada novo nó de storage, especialmente se os nós de storage existentes contiverem uma grande quantidade de metadados de objetos.

Adicionar novo site

Se você estiver adicionando um novo site, use `nodetool status` para monitorar o progresso do fluxo do Cassandra e para ver a quantidade de metadados que foram copiados para o novo site durante o estágio "expandindo o cluster do Cassandra". A carga total de dados no novo site deve estar dentro de cerca de 20% do total de um site atual.



Não reinicie nenhum nó de storage durante os estágios "expandindo o cluster Cassandra" ou "iniciando Cassandra e streaming de dados". Esses estágios podem levar muitas horas para serem concluídos para cada novo nó de storage, especialmente se os nós de storage existentes contiverem uma grande quantidade de metadados de objetos.

1. Continue monitorando a expansão até que todas as tarefas estejam concluídas e o botão **Configurar expansão** reapareça.

Depois de terminar

Dependendo dos tipos de nós de grade adicionados, você deve executar etapas adicionais de integração e configuração. [Etapas de configuração após a expansão](#) Consulte .

Configurar o sistema expandido

Etapas de configuração após a expansão

Depois de concluir uma expansão, você deve executar etapas adicionais de integração e configuração.

Sobre esta tarefa

Você deve concluir as tarefas de configuração listadas abaixo para os nós de grade que você está adicionando em sua expansão. Algumas tarefas podem ser opcionais, dependendo das opções selecionadas durante a instalação e administração do sistema, e como você deseja configurar os nós de grade adicionados durante a expansão.

Passos

1. Se você adicionou um nó de storage, execute as seguintes tarefas de configuração:
 - a. Revise os pools de armazenamento usados em suas regras de ILM para garantir que o novo armazenamento será usado. [Gerenciar objetos com ILM](#)Consulte .
 - Se você adicionou um site, crie um pool de armazenamento para o site e atualize as regras do ILM para usar o novo pool de armazenamento.
 - Se você adicionou um nó de armazenamento a um site existente, confirme se o novo nó usa o grau de armazenamento correto.



Por padrão, um novo nó de storage é atribuído ao nível de storage de todos os nós de storage e adicionado a pools de storage que usam esse nível para o site. Se você quiser que um novo nó use um grau de armazenamento personalizado, você deve atribuí-lo manualmente ao grau personalizado (**ILM > graus de armazenamento**).

- b. Verifique se o nó de armazenamento está ingerindo objetos. [Verifique se o nó de storage está ativo](#)Consulte .
 - c. Rebalancear os dados codificados por apagamento (somente se você não conseguir adicionar o número recomendado de nós de storage). [Rebalancear os dados codificados por apagamento após adicionar nós de storage](#)Consulte .
2. Se você adicionou um nó de gateway, execute a seguinte tarefa de configuração:
 - Se os grupos de alta disponibilidade (HA) forem usados para conexões de cliente, adicione opcionalmente o nó de gateway a um grupo de HA. Selecione **CONFIGURATION > Network > High Availability Groups** para rever a lista de grupos de HA existentes e adicionar o novo nó. [Administrar o StorageGRID](#)Consulte .
 3. Se você adicionou um nó Admin, execute as seguintes tarefas de configuração:
 - a. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID, crie uma confiança de parte confiável para o novo nó de administração. Você não pode entrar no nó até criar essa confiança de parte confiável. [Configurar o logon único](#)Consulte .
 - b. Se você planeja usar o serviço Load Balancer em nós de administração, adicione opcionalmente o novo nó de administração a um grupo de HA. Selecione **CONFIGURATION > Network > High Availability Groups** para rever a lista de grupos de HA existentes e adicionar o novo nó. [Administrar o StorageGRID](#)Consulte .
 - c. Opcionalmente, copie o banco de dados do nó Admin do nó Admin principal para o nó Admin de expansão se quiser manter as informações de atributo e auditoria consistentes em cada nó Admin.

[Copie o banco de dados Admin Node](#)Consulte .

- d. Opcionalmente, copie o banco de dados Prometheus do nó Admin primário para o nó Admin de expansão se quiser manter as métricas históricas consistentes em cada nó Admin. [Copiar métricas Prometheus](#)Consulte .
- e. Opcionalmente, copie os logs de auditoria existentes do nó de administração principal para o nó de administração de expansão se quiser manter as informações de log histórico consistentes em cada nó de administração. [Copiar registros de auditoria](#)Consulte .
- f. Opcionalmente, configure o acesso ao sistema para fins de auditoria por meio de um compartilhamento de arquivos NFS ou CIFS. [Administrar o StorageGRID](#)Consulte .



A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

- g. Opcionalmente, altere o remetente preferido para notificações. Você pode tornar o nó de administração de expansão o remetente preferido. Caso contrário, um nó de administração existente configurado como o remetente preferido continua a enviar notificações, incluindo mensagens AutoSupport, notificações SNMP, e-mails de alerta e e-mails de alarme (sistema legado). [Administrar o StorageGRID](#)Consulte .
4. Se tiver adicionado um nó de arquivo, conclua as seguintes tarefas de configuração.
- a. Configure a ligação do nó de arquivo ao sistema de armazenamento de arquivo externo de destino. Quando você conclui a expansão, os nós de arquivo estão em um estado de alarme até que você configure as informações de conexão através do componente **ARC > Target**. [Administrar o StorageGRID](#)Consulte .
 - b. Atualize a política ILM para arquivar dados de objetos através do novo nó de arquivo. [Gerenciar objetos com ILM](#)Consulte .
 - c. Configure alarmes personalizados para os atributos usados para monitorar a velocidade e a eficiência da recuperação de dados de objetos a partir de nós de arquivo. [Administrar o StorageGRID](#)Consulte .
5. Para verificar se os nós de expansão foram adicionados a uma rede cliente não confiável ou para alterar se a rede cliente de um nó não é confiável ou confiável, vá para **CONFIGURATION > Network > UnTrusted Client Network**.

Se a rede do cliente no nó de expansão não for confiável, as conexões com o nó na rede do cliente devem ser feitas usando um ponto de extremidade do balanceador de carga. [Administrar o StorageGRID](#)Consulte .

6. Configure o sistema de nomes de domínio (DNS).

Se você tiver especificado as configurações de DNS separadamente para cada nó de grade, você deve adicionar configurações de DNS personalizadas por nó para os novos nós. [Modifique a configuração DNS para um nó de grade único](#)Consulte .

A melhor prática é que a lista de servidores DNS em toda a grade contenha alguns servidores DNS que são acessíveis localmente a partir de cada site. Se você acabou de adicionar um novo site, adicione novos servidores DNS para o site à configuração DNS em toda a grade.



Forneça dois a seis endereços IPv4 para servidores DNS. Você deve selecionar servidores DNS que cada site pode acessar localmente no caso de rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode personalizar ainda mais a lista de servidores DNS para cada nó. Para obter detalhes, [Modifique a configuração DNS para um nó de grade único](#) consulte ..

7. Se você adicionou um novo site, confirme se os servidores NTP (Network Time Protocol) estão acessíveis a partir desse site. [Configurar servidores NTP](#) Consulte .



Certifique-se de que pelo menos dois nós em cada local possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um local puder alcançar as fontes NTP, problemas de tempo ocorrerão se esse nó cair. Além disso, a designação de dois nós por local como fontes primárias de NTP garante um tempo preciso se um local for isolado do resto da grade.

Verifique se o nó de storage está ativo

Após a conclusão de uma operação de expansão que adiciona novos nós de storage, o sistema StorageGRID deve começar a usar automaticamente os novos nós de storage. Você deve usar o sistema StorageGRID para verificar se o novo nó de storage está ativo.

Passos

1. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
2. Selecione **NÓS > Expansion Storage Node > Storage**.
3. Passe o cursor sobre o gráfico **Storage Used - Object Data** (armazenamento usado - dados do objeto) para visualizar o valor para **Used**, que é a quantidade total de espaço utilizável que foi usada para dados do objeto.
4. Verifique se o valor de **usado** está aumentando à medida que você move o cursor para a direita no gráfico.

Copiar base de dados Admin Node

Ao adicionar nós de administração através de um procedimento de expansão, você pode opcionalmente copiar o banco de dados do nó de administração principal para o novo nó de administração. Copiar o banco de dados permite que você retenha informações históricas sobre atributos, alertas e alertas.

O que você vai precisar

- Você concluiu as etapas de expansão necessárias para adicionar um nó de administrador.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

O processo de ativação do software StorageGRID cria um banco de dados vazio para o serviço NMS no nó de administração de expansão. Quando o serviço NMS é iniciado no nó de administração de expansão, ele registra informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados mais tarde. Este banco de dados Admin Node inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **SUPPORT > Tools > Grid topology**

Para garantir que o banco de dados do nó de administração seja consistente entre nós, você pode copiar o banco de dados do nó de administração principal para o nó de administração de expansão.



Copiar o banco de dados do nó Admin principal (o nó *Adminsource*) para um nó Admin de expansão pode levar até várias horas para ser concluído. Durante esse período, o Gerenciador de Grade fica inacessível.

Siga estas etapas para interromper o serviço MI e o serviço API de gerenciamento no nó de administração principal e no nó de administração de expansão antes de copiar o banco de dados.

Passos

1. Conclua as etapas a seguir no nó de administração principal:
 - a. Faça login no nó Admin:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Execute o seguinte comando: `recover-access-points`
 - c. Introduza a frase-passe de aprovisionamento.
 - d. Parar o serviço MI: `service mi stop`
 - e. Pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
2. Execute as seguintes etapas no nó de administração de expansão:
 - a. Faça login no nó de administração de expansão:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Parar o serviço MI: `service mi stop`
 - c. Pare o serviço mgmt-api: `service mgmt-api stop`
 - d. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
 - e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - f. Copie o banco de dados do nó Admin de origem para o nó Admin de expansão:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando solicitado, confirme se deseja substituir o banco de dados MI no nó de administração de expansão.

O banco de dados e seus dados históricos são copiados para o nó de administração de expansão. Quando a operação de cópia é concluída, o script inicia o nó de administração de expansão.

h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`

3. Reinicie os serviços no nó de administração principal: `service servermanager start`

Copiar métricas Prometheus

Depois de adicionar um novo nó Admin, você pode opcionalmente copiar as métricas históricas mantidas pelo Prometheus do nó Admin primário para o novo nó Admin. Copiar as métricas garante que as métricas históricas sejam consistentes entre os nós de administração.

O que você vai precisar

- O novo Admin Node está instalado e em execução.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Quando você adiciona um Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Você pode manter as métricas históricas consistentes entre nós copiando o banco de dados Prometheus do nó Admin primário (o *source Admin Node*) para o novo Admin Node.



Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

Passos

1. Faça login no nó de administração de origem:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Conclua as etapas a seguir no novo nó Admin:
 - a. Faça login no novo nó Admin:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Pare o serviço Prometheus: `service prometheus stop`

- c. Adicione a chave privada SSH ao agente SSH. Introduza:`ssh-add`
- d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
- e. Copie o banco de dados Prometheus do nó Admin de origem para o novo nó Admin:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no novo nó Admin.

O banco de dados Prometheus original e seus dados históricos são copiados para o novo Admin Node. Quando a operação de cópia é concluída, o script inicia o novo Admin Node. É apresentado o seguinte estado:

```
Database cloned, starting services
```

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:

```
ssh-add -D
```

4. Reinicie o serviço Prometheus no Admin Node de origem.

```
service prometheus start
```

Copiar registros de auditoria

Quando você adiciona um novo nó Admin por meio de um procedimento de expansão, seu serviço AMS somente Registra eventos e ações que ocorrem depois que ele se une ao sistema. Conforme necessário, você pode copiar logs de auditoria de um nó de administrador instalado anteriormente para o novo nó de administração de expansão, de modo que ele esteja sincronizado com o resto do sistema StorageGRID.

O que você vai precisar

- Você concluiu as etapas de expansão necessárias para adicionar um nó de administrador.
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Para disponibilizar mensagens de auditoria histórica em um novo nó de administração, você deve copiar os arquivos de log de auditoria manualmente de um nó de administração existente para o nó de administração de expansão.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode ignorar estas etapas se qualquer uma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para nós de administrador.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

[Configurar mensagens de auditoria e destinos de log](#) Consulte para obter detalhes.

Passos

1. Faça login no nó de administração principal:

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

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

2. Pare o serviço AMS para impedir que ele crie um novo arquivo: `service ams stop`

3. Renomeie `audit.log` o arquivo para garantir que ele não substitua o arquivo no nó de administração de expansão para o qual você está copiando:

```
cd /var/local/audit/export ls -l E mv audit.log new_name.txt
```

4. Copiar todos os arquivos de log de auditoria para o nó de administração de expansão:

```
scp -p * IP_address:/var/local/audit/export
```

5. Se for solicitada a senha para `/root/.ssh/id_rsa`, digite a senha de acesso SSH para o nó de administração principal listado no `Passwords.txt` arquivo.

6. Restaure o arquivo original `audit.log`:

```
mv new_name.txt audit.log
```

7. Inicie o serviço AMS:

```
service ams start
```

8. Terminar sessão a partir do servidor:

```
exit
```

9. Faça login no nó de administração de expansão:

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

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

10. Atualize as configurações de usuário e grupo para os arquivos de log de auditoria:

```
cd /var/local/audit/export E chown ams-user:bycast *
```

11. Terminar sessão a partir do servidor:

Rebalancear os dados codificados por apagamento após adicionar nós de storage

Em alguns casos, talvez você precise rebalancear os dados codificados por apagamento após adicionar novos nós de storage.

O que você vai precisar

- Você concluiu as etapas de expansão para adicionar os novos nós de storage.
- Você revisou o [considerações para rebalanceamento de dados codificados por apagamento](#).



Execute este procedimento somente se o alerta **armazenamento de objetos baixos** tiver sido acionado para um ou mais nós de armazenamento em um local e você não conseguir adicionar o número recomendado de novos nós de armazenamento.

- Você entende que os dados de objeto replicados não serão movidos por este procedimento e que o procedimento de rebalancear EC não considera o uso de dados replicados em cada nó de storage ao determinar onde mover dados codificados por apagamento.
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Quando o procedimento de reequilíbrio EC está em execução, o desempenho das operações ILM e das operações dos clientes S3 e Swift provavelmente serão impactados. Por esse motivo, você só deve executar esse procedimento em casos limitados.



O procedimento de reequilíbrio CE reserva temporariamente uma grande quantidade de armazenamento. Os alertas de storage podem ser acionados, mas serão resolvidos quando o rebalancear for concluído. Se não houver armazenamento suficiente para a reserva, o procedimento de reequilíbrio CE falhará. As reservas de armazenamento são liberadas quando o procedimento de reequilíbrio CE for concluído, independentemente de o procedimento ter falhado ou ter êxito.



As operações S3 e Swift API para carregar objetos (ou partes de objetos) podem falhar durante o procedimento de rebalanceamento EC se precisarem de mais de 24 horas para serem concluídas. As OPERAÇÕES PUT de longa duração falharão se a regra ILM aplicável usar um posicionamento rigoroso ou equilibrado na ingestão. Será comunicado o seguinte erro:

```
500 Internal Server Error
```

Passos

1. Revise os detalhes de armazenamento de objetos atuais para o site que você planeja reequilibrar.
 - a. Selecione **NODES**.
 - b. Selecione o primeiro nó de storage no local.
 - c. Selecione a guia **armazenamento**.
 - d. Passe o cursor sobre o gráfico Storage Used - Object Data (armazenamento usado - dados de objetos) para ver a quantidade atual de dados replicados e dados codificados por apagamento no Storage Node.
 - e. Repita estas etapas para exibir os outros nós de storage no local.

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. Introduza o seguinte comando:

```
rebalance-data start --site "site-name"
```

Para "`site-name`", especifique o primeiro local em que você adicionou novos nós ou nós de storage. Inclua `site-name` em citações.

O procedimento de reequilíbrio EC é iniciado e um ID de tarefa é retornado.

4. Copie a ID do trabalho.

5. Acompanhar o estado do procedimento de reequilíbrio CE.

- Para visualizar o estado de um procedimento único de reequilíbrio CE:

```
rebalance-data status --job-id job-id
```

Para `job-id`, especifique o ID que foi retornado quando você iniciou o procedimento.

- Para visualizar o estado do atual procedimento de reequilíbrio CE e de quaisquer procedimentos concluídos anteriormente:

```
rebalance-data status
```



Para obter ajuda sobre o comando `rebalanceamento-data`:

```
rebalance-data --help
```

- Para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual, selecione **support > Tools > Metrics**. Em seguida, selecione **EC Overview** na seção Grafana. Veja os painéis **Grid EC Job tempo estimado para conclusão** e **Grid EC Job percentage Completed**.

6. Execute etapas adicionais, com base no status retornado:

- Se o estado indicar `In progress`, a operação de reequilíbrio CE continua a funcionar. Você deve monitorar periodicamente o procedimento até que ele seja concluído.
- Se o estado indicar `Failure`, efetuar o [passos de falha](#).
- Se o estado indicar `Success`, efetuar o [etapa de sucesso](#).

7. Se o procedimento de reequilíbrio EC estiver gerando muita carga (por exemplo, as operações de ingestão são afetadas), interrompa o procedimento.

```
rebalance-data pause --job-id job-id
```

8. Se você precisar encerrar o procedimento de rebalanceamento EC (por exemplo, para que você possa executar uma atualização de software StorageGRID), digite o seguinte:

```
rebalance-data terminate --job-id job-id
```



Quando você encerrar um procedimento de rebalanceamento do EC, todos os fragmentos de dados que já foram movidos permanecem no novo local. Os dados não são movidos de volta para o local original.

9. se o status do procedimento EC Rebalanceance for `Failure`, siga estas etapas:

- Confirme se todos os nós de storage no local estão conectados à grade.
- Verifique e resolva quaisquer alertas que possam estar afetando esses nós de storage.

Para obter informações sobre alertas específicos, consulte as instruções de monitoramento e solução de problemas.

- Reinicie o procedimento de reequilíbrio CE `rebalance-data start --job-id job-id`

- Se o estado do procedimento de reequilíbrio CE persistir `Failure`, contactar o suporte técnico.

10. se o status do procedimento de rebalanceamento EC for `Success`, opcionalmente [revise o armazenamento de objetos](#) para ver os detalhes atualizados do local.

Agora, os dados codificados por apagamento devem ser mais equilibrados entre os nós de storage no local.

11. Se você estiver usando codificação de apagamento em mais de um site, execute este procedimento para todos os outros sites afetados.

Entre em Contato com o suporte técnico

Se você encontrar erros durante o processo de expansão da grade que você não consegue resolver ou se uma tarefa de grade falhar, entre em Contato com o suporte técnico.

Sobre esta tarefa

Ao entrar em Contato com o suporte técnico, você deve fornecer os arquivos de log necessários para ajudar a solucionar os erros que você está encontrando.

Passos

- Conecte-se ao nó de expansão que sofreu falhas:

- Introduza o seguinte comando: `ssh -p 8022 admin@grid_node_IP`



A porta 8022 é a porta SSH do sistema operacional base, enquanto a porta 22 é a porta SSH do mecanismo de contentor que executa o StorageGRID.

- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Depois de iniciar sessão como root, o aviso muda de \$ para #.

2. Dependendo do estágio em que a instalação chegou, recupere qualquer um dos seguintes logs que estão disponíveis no nó da grade:

Plataforma	Registos
VMware	<ul style="list-style-type: none">• /var/log/daemon.log• /var/log/storagegrid/daemon.log• /var/log/storagegrid/nodes/<node-name>.log
Linux	<ul style="list-style-type: none">• /var/log/storagegrid/daemon.log• /etc/storagegrid/nodes/<node-name>.conf (para cada nó com falha)• /var/log/storagegrid/nodes/<node-name>.log (para cada nó com falha; pode não existir)

Recuperar e manter

Recuperar e manter: Visão geral

Use estas instruções para manter seu sistema StorageGRID e para se recuperar de falhas.

Sobre estas instruções

Estas instruções descrevem como aplicar um hotfix de software, recuperar nós de grade, recuperar um site com falha, desativar nós de grade ou um site inteiro, executar manutenção de rede, executar procedimentos de manutenção de nível de host e middleware e executar procedimentos de nó de grade.



Nestas instruções, "Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Utilize o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" para obter uma lista de versões suportadas.

Antes de começar

- Você tem uma ampla compreensão do sistema StorageGRID.
- Você revisou a topologia do seu sistema StorageGRID e entende a configuração da grade.
- Você entende que deve seguir todas as instruções exatamente e atender a todos os avisos.
- Você entende que os procedimentos de manutenção não descritos não são suportados ou exigem um envolvimento dos serviços.

Procedimentos de manutenção para aparelhos

Para obter os procedimentos de hardware, consulte as instruções de instalação e manutenção do seu dispositivo StorageGRID.

- [Aparelhos de serviços SG100 e SG1000](#)
- [SG6000 dispositivos de armazenamento](#)
- [SG5700 dispositivos de armazenamento](#)
- [SG5600 dispositivos de armazenamento](#)

Baixar Recovery Package

O arquivo do pacote de recuperação permite restaurar o sistema StorageGRID se ocorrer uma falha.

O que você vai precisar

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

Faça o download do arquivo atual do Pacote de recuperação antes de fazer alterações na topologia da grade no sistema StorageGRID ou antes de atualizar o software. Em seguida, faça o download de uma nova cópia do Pacote de recuperação após fazer alterações na topologia da grade ou após atualizar o software.

Passos

1. Selecione **MAINTENANCE > System > Recovery package**.
2. Digite a senha de provisionamento e selecione **Iniciar download**.

O download começa imediatamente.

3. Quando o download for concluído:
 - a. Abra o `.zip` ficheiro.
 - b. Confirme que inclui um diretório `gpt-backup` e um arquivo interno `.zip`.
 - c. Extraia o arquivo interno `.zip`.
 - d. Confirme que você pode abrir o `Passwords.txt` arquivo.
4. Copie o arquivo do pacote de recuperação baixado (`.zip`) para dois locais seguros, seguros e separados.



O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

Informações relacionadas

[Administrar o StorageGRID](#)

Procedimento de correção do StorageGRID

Talvez seja necessário aplicar um hotfix ao seu sistema StorageGRID se problemas com o software forem detetados e resolvidos entre versões de recursos.

Os hotfixes do StorageGRID contêm alterações de software que são disponibilizadas fora de uma versão de recurso ou patch. As mesmas alterações estão incluídas em uma versão futura. Além disso, cada versão de hotfix contém um roll-up de todos os hotfixes anteriores dentro da versão de recurso ou patch.

Considerações para aplicar um hotfix

Quando você aplica um hotfix, uma série cumulativa de atualizações de software é aplicada aos nós do seu sistema StorageGRID.

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver sendo executado. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação está sendo executado.



Se um procedimento de desativação de nó ou site estiver pausado, você pode aplicar um hotfix com segurança. Além disso, você pode ser capaz de aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Consulte as instruções para atualizar o software StorageGRID para obter detalhes.

Depois de carregar o hotfix no Gerenciador de Grade, o hotfix é aplicado automaticamente ao nó de administrador principal. Em seguida, você pode aprovar o aplicativo do hotfix para o resto dos nós no seu sistema StorageGRID.

Se um hotfix não for aplicado a um ou mais nós, o motivo da falha será exibido na coluna Detalhes da tabela de progresso do hotfix. Você deve resolver quaisquer problemas que causaram as falhas e, em seguida, tentar novamente todo o processo. Os nós com uma aplicação anteriormente bem-sucedida do hotfix serão ignorados nos aplicativos subsequentes. Você pode tentar novamente o processo de hotfix com segurança quantas vezes for necessário até que todos os nós tenham sido atualizados. O hotfix deve ser instalado com sucesso em todos os nós de grade para que o aplicativo seja concluído.

Embora os nós de grade sejam atualizados com a nova versão de hotfix, as alterações reais em um hotfix podem afetar apenas serviços específicos em tipos específicos de nós. Por exemplo, um hotfix pode afetar apenas o serviço LDR em nós de armazenamento.

Como os hotfixes são aplicados para recuperação e expansão

Depois que um hotfix foi aplicado à sua grade, o nó de administrador principal instala automaticamente a mesma versão de hotfix para todos os nós restaurados por operações de recuperação ou adicionados em uma expansão.

No entanto, se você precisar recuperar o nó de administração principal, você deve instalar manualmente a versão correta do StorageGRID e, em seguida, aplicar o hotfix. A versão final do StorageGRID do nó de administração principal deve corresponder à versão dos outros nós na grade.

O exemplo a seguir ilustra como aplicar um hotfix ao recuperar o nó de administrador principal:

1. Suponha que a grade esteja executando uma versão do StorageGRID 11.A.B com o hotfix mais recente. A "versão em grade" é 11.A.B.y.
2. O nó de administração principal falha.
3. Reimplante o nó de administração principal usando o StorageGRID 11.A.B e execute o procedimento de recuperação.



Conforme necessário para corresponder à versão da grade, você pode usar uma versão menor ao implantar o nó; você não precisa implantar a versão principal primeiro.

4. Em seguida, aplique o hotfix 11.A.B.y ao nó de administração principal.

Informações relacionadas

Planeje e prepare-se para um hotfix

Você deve Planejar antes de aplicar um hotfix para garantir uma interrupção mínima ao seu sistema StorageGRID.

Passos

- [Como seu sistema é afetado quando você aplica um hotfix](#)
- [Obter os materiais necessários para um hotfix](#)
- [Transferir o ficheiro de correção](#)
- [Verificar a condição do sistema antes de aplicar um hotfix](#)

Como seu sistema é afetado quando você aplica um hotfix

Você deve entender como seu sistema StorageGRID será afetado quando você aplicar um hotfix.

As aplicações do cliente podem sofrer interrupções de curto prazo

O sistema StorageGRID pode obter e recuperar dados de aplicativos clientes durante todo o processo de hotfix; no entanto, as conexões de clientes com nós de gateway individuais ou nós de armazenamento podem ser interrompidas temporariamente se o hotfix precisar reiniciar os serviços nesses nós. A conectividade será restaurada após a conclusão do processo de correção e os serviços são retomados nos nós individuais.

Talvez seja necessário agendar o tempo de inatividade para aplicar um hotfix se a perda de conectividade por um curto período não for aceitável. Você pode usar a aprovação seletiva para agendar quando certos nós são atualizados.



Você pode usar vários gateways e grupos de alta disponibilidade (HA) para fornecer failover automático durante o processo de hotfix. Consulte as instruções para [configurando grupos de alta disponibilidade](#).

Alertas e notificações SNMP podem ser acionados

Alertas e notificações SNMP podem ser acionados quando os serviços são reiniciados e quando o sistema StorageGRID está operando como um ambiente de versão mista (alguns nós de grade executando uma versão anterior, enquanto outros foram atualizados para uma versão posterior). Em geral, esses alertas e notificações serão apagados quando o hotfix for concluído.

As alterações de configuração são restritas

Ao aplicar um hotfix ao StorageGRID:

- Não faça alterações na configuração da grade (por exemplo, especificando sub-redes de rede de grade ou aprovando nós de grade pendentes) até que o hotfix tenha sido aplicado a todos os nós.
- Não atualize a configuração do ILM até que o hotfix tenha sido aplicado a todos os nós.

Obtenha os materiais necessários para o hotfix

Antes de aplicar um hotfix, você deve obter todos os materiais necessários.

Item	Notas
Ficheiro de correção do StorageGRID	Você deve baixar o arquivo de hotfix do StorageGRID.
<ul style="list-style-type: none"> • Porta de rede • Navegador da Web suportado • Cliente SSH (por exemplo, PuTTY) 	
Pacote de recuperação (.zip) arquivo	Antes de aplicar um hotfix, Baixe o mais recente arquivo de pacote de recuperação no caso de ocorrer algum problema durante o hotfix. Então, após a aplicação do hotfix, baixe uma nova cópia do arquivo do pacote de recuperação e salve-o em um local seguro. O arquivo atualizado do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.
Ficheiro Passwords.txt	Opcional e usado somente se você estiver aplicando um hotfix manualmente usando o cliente SSH. O Passwords.txt arquivo está incluído no REFERIDO pacote, que faz parte do arquivo Recovery Package .zip.
Frase-passe do provisionamento	A frase-passe é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está listada no Passwords.txt arquivo.
Documentação relacionada	readme.txt ficheiro para a correção. Este arquivo está incluído na página de download do hotfix. Certifique-se de rever o readme ficheiro cuidadosamente antes de aplicar a correção.

Informações relacionadas

[Transfira o ficheiro de correção](#)

Transfira o ficheiro de correção

Tem de transferir o ficheiro de correção para poder aplicar a correção.

Passos

1. Vá para a página de downloads do NetApp para StorageGRID.

["NetApp Downloads: StorageGRID"](#)

2. Selecione a seta para baixo em **Software disponível** para ver uma lista de hotfixes disponíveis para download.



As versões do arquivo de hotfix têm o formulário: 11,4.x.y.

3. Reveja as alterações incluídas na atualização.



Se você acabou de recuperar o nó de administrador principal e precisa aplicar um hotfix, selecione a mesma versão de hotfix que está instalada nos outros nós de grade.

- a. Selecione a versão do hotfix que deseja baixar e selecione **Go**.
- b. Inicie sessão utilizando o nome de utilizador e a palavra-passe da sua conta NetApp.
- c. Leia e aceite o Contrato de Licença de Usuário final.

É apresentada a página de transferência da versão selecionada.

- d. Transfira o ficheiro de correção `readme.txt` para ver um resumo das alterações incluídas na correção.
4. Selecione o botão de download do hotfix e salve o arquivo.



Não altere o nome deste ficheiro.



Se você estiver usando um dispositivo macOS, o arquivo de hotfix pode ser salvo automaticamente como um `.txt` arquivo. Se estiver, você deve renomear o arquivo sem a `.txt` extensão.

5. Selecione um local para o download e selecione **Salvar**.

Informações relacionadas

[Configure o nó de administração principal de substituição](#)

Verifique a condição do sistema antes de aplicar o hotfix

Você deve verificar se o sistema está pronto para acomodar o hotfix.

1. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
2. Se possível, verifique se o sistema está funcionando normalmente e se todos os nós da grade estão conectados à grade.

Os nós conectados têm marcas de verificação verdes  na página nós.

3. Verifique e resolva quaisquer alertas atuais, se possível.

Para obter informações sobre alertas específicos, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

4. Certifique-se de que não existem outros procedimentos de manutenção em curso, como um procedimento de atualização, recuperação, expansão ou desativação.

Você deve esperar que todos os procedimentos de manutenção ativos sejam concluídos antes de aplicar um hotfix.

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver sendo executado. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação está sendo executado.



Se um procedimento de desativação de nó ou site estiver pausado, você pode aplicar um hotfix com segurança. Além disso, você pode ser capaz de aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Consulte as instruções para atualizar o software StorageGRID para obter detalhes.

Informações relacionadas

[Monitorar e solucionar problemas](#)

[Pausar e retomar o processo de desativação dos nós de storage](#)

Aplicar hotfix

A correção é aplicada automaticamente primeiro ao nó de administração principal. Em seguida, você deve aprovar o aplicativo do hotfix para outros nós de grade até que todos os nós estejam executando a mesma versão de software. Você pode personalizar a sequência de aprovação selecionando para aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

O que você vai precisar

- Você revisou as considerações e concluiu as etapas em [Planeje e prepare-se para um hotfix](#).
- Você tem a senha de provisionamento.
- Você tem acesso root ou a permissão Manutenção.

Sobre esta tarefa

- Pode atrasar a aplicação de uma correção a um nó, mas o processo de correção não está concluído até aplicar a correção a todos os nós.
- Não é possível executar uma atualização do software StorageGRID ou uma atualização do SANtricity os até que tenha concluído o processo de correção.

Passos

1. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
2. Selecione **MAINTENANCE > System > Software update**.

A página Atualização de software é exibida.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances.

StorageGRID upgrade Upgrade to the next StorageGRID version and apply the latest hotfix for that version. Upgrade →	StorageGRID hotfix Apply a hotfix to your current StorageGRID software version. Apply hotfix →	SANtricity OS update Update the SANtricity OS software on your StorageGRID storage appliances. Update →
--	---	--

3. Selecione **aplicar hotfix**.

A página de correção do StorageGRID é exibida.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available. When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Passphrase

Provisioning Passphrase ?

4. Selecione o ficheiro de correção transferido a partir do site de suporte da NetApp.

- Selecione **Procurar**.
- Localize e selecione o ficheiro.

`hotfix-install-version`

- Selecione **Open**.

O ficheiro é carregado. Quando o upload estiver concluído, o nome do arquivo é mostrado no campo Detalhes.



Não altere o nome do arquivo, pois ele faz parte do processo de verificação.

5. Insira a senha de provisionamento na caixa de texto.

O botão **Start** (Iniciar) fica ativado.

6. Selecione **Iniciar**.

É apresentado um aviso informando que a ligação do seu browser pode ser perdida temporariamente à medida que os serviços no nó de administração principal são reiniciados.

Warning

Connection Might be Temporarily Lost

When the hotfix is applied, your browser's connection might be lost temporarily as services on the primary Admin Node are stopped and restarted. Are you sure you want to start the hotfix installation process?

Cancel

OK

7. Selecione **OK** para começar a aplicar o hotfix ao nó de administração principal.

Quando o hotfix é iniciado:

a. As validações de hotfix são executadas.



Se algum erro for relatado, resolva-os, faça o upload novamente do arquivo de hotfix e selecione **Iniciar** novamente.

b. A tabela de progresso da instalação do hotfix é exibida. Esta tabela mostra todos os nós na grade e o estágio atual da instalação do hotfix para cada nó. Os nós da tabela são agrupados por tipo:

- Nós de administração
- Nós de gateway
- Nós de storage
- Nós de arquivamento



A barra de progresso atinge a conclusão e, em seguida, o nó de administração principal é mostrado primeiro com o estágio "concluído".

Approve All
Remove All

Admin Nodes - 1 out of 1 completed

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

8. Opcionalmente, classifique as listas de nós em cada agrupamento em ordem crescente ou decrescente por **Site**, **Nome**, **progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **pesquisar** para pesquisar nós específicos.
9. Aprove os nós de grade que estão prontos para ser atualizados. Nós aprovados do mesmo tipo são atualizados um de cada vez.



Não aprove o hotfix para um nó, a menos que você tenha certeza de que o nó está pronto para ser atualizado. Quando o hotfix for aplicado a um nó de grade, alguns serviços nesse nó podem ser reiniciados. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

- Selecione um ou mais botões **Approve** para adicionar um ou mais nós individuais à fila de correções.
- Selecione o botão **Approve All** em cada agrupamento para adicionar todos os nós do mesmo tipo à fila de correções. Se você inseriu critérios de pesquisa na caixa **pesquisar**, o botão **aprovar tudo** se aplica a todos os nós selecionados pelos critérios de pesquisa.



O botão **Approve All** na parte superior da página aprova todos os nós listados na página, enquanto o botão **Approve All** na parte superior de um agrupamento de tabelas só aprova todos os nós nesse grupo. Se a ordem em que os nós são atualizados for importante, aprove nós ou grupos de nós um de cada vez e aguarde até que a atualização seja concluída em cada nó antes de aprovar o(s) próximo(s) nó(s).

- Selecione o botão de nível superior **Approve All** na parte superior da página para adicionar todos os nós na grade à fila de hotfix.



Tem de concluir a correção do StorageGRID antes de poder iniciar uma atualização de software diferente. Se não conseguir concluir a correção, contacte o suporte técnico.

- Selecione **Remove** ou **Remove tudo** para remover um nó ou todos os nós da fila de correções.

Quando o estágio progride além de "enfileirado", o botão **Remove** fica oculto e você não pode mais remover o nó do processo de hotfix.

Storage Nodes - 1 out of 9 completed

Approve All Remove All

Search

Site	Name	Progress	Stage	Details	Action
Raleigh	RAL-S1-101-196		Queued		Remove
Raleigh	RAL-S2-101-197		Complete		
Raleigh	RAL-S3-101-198		Queued		Remove
Sunnyvale	SVL-S1-101-199		Queued		Remove
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		Approve
Sunnyvale	SVL-S3-101-94		Waiting for you to approve		Approve
Vancouver	VTC-S1-101-193		Waiting for you to approve		Approve
Vancouver	VTC-S2-101-194		Waiting for you to approve		Approve
Vancouver	VTC-S3-101-195		Waiting for you to approve		Approve

10. Aguarde enquanto o hotfix é aplicado a cada nó de grade aprovado.

Quando o hotfix tiver sido instalado com sucesso em todos os nós, a tabela de progresso da instalação do Hotfix será fechada. Um banner verde mostra a data e a hora em que o hotfix foi concluído.

11. Se o hotfix não puder ser aplicado a nenhum nó, revise o erro de cada nó, resolva o problema e repita essas etapas.

O procedimento não está concluído até que o hotfix seja aplicado com êxito a todos os nós. Você pode tentar novamente o processo de hotfix com segurança quantas vezes for necessário até que ele seja concluído.

Informações relacionadas

[Administrar o StorageGRID](#)

[Monitorar e solucionar problemas](#)

Procedimentos de recuperação do nó de grade

Se um nó de grade falhar, você poderá recuperá-lo substituindo o servidor físico ou virtual com falha, reinstalando o software StorageGRID e restaurando dados recuperáveis.

Os nós de grade podem falhar se uma falha de hardware, virtualização, sistema operacional ou software tornar o nó inoperável ou não confiável. Há muitos tipos de falha que podem desencadear a necessidade de recuperar um nó de grade.

As etapas para recuperar um nó de grade variam, dependendo da plataforma onde o nó de grade está hospedado e do tipo de nó de grade. Cada tipo de nó de grade tem um procedimento de recuperação específico, que você deve seguir exatamente.

Geralmente, você tenta preservar os dados do nó de grade com falha quando possível, reparar ou substituir o nó com falha, usar o Gerenciador de Grade para configurar o nó de substituição e restaurar os dados do nó.



Se um site StorageGRID inteiro falhar, entre em Contato com o suporte técnico. O suporte técnico trabalhará com você para desenvolver e executar um plano de recuperação de local que maximiza a quantidade de dados recuperados e atende aos seus objetivos de negócios.

Informações relacionadas

[Como a recuperação do local é realizada pelo suporte técnico](#)

Avisos e considerações para a recuperação do nó da grade

Se um nó de grade falhar, você deve recuperá-lo o mais rápido possível. Você deve rever todos os avisos e considerações sobre a recuperação do nó antes de começar.



O StorageGRID é um sistema distribuído composto por vários nós que trabalham uns com os outros. Não use snapshots de disco para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção para cada tipo de nó.

Alguns dos motivos para recuperar um nó de grade com falha o mais rápido possível incluem o seguinte:

- Um nó de grade com falha pode reduzir a redundância de dados do sistema e do objeto, deixando você vulnerável ao risco de perda permanente de dados se outro nó falhar.
- Um nó de grade com falha pode afetar a eficiência das operações diárias.
- Um nó de grade com falha pode reduzir sua capacidade de monitorar as operações do sistema.
- Um nó de grade com falha pode causar um erro de servidor interno do 500 se regras rígidas de ILM estiverem em vigor.
- Se um nó de grade não for recuperado prontamente, os tempos de recuperação podem aumentar. Por exemplo, podem ocorrer filas que precisam ser limpas antes da conclusão da recuperação.

Siga sempre o procedimento de recuperação para o tipo específico de nó de grade que você está recuperando. Os procedimentos de recuperação variam para nós de administração primários ou não primários, nós de gateway, nós de arquivamento, nós de dispositivo e nós de storage.

Pré-condições para a recuperação de nós de grade

Todas as condições a seguir são assumidas ao recuperar nós de grade:

- O hardware físico ou virtual com falha foi substituído e configurado.
- A versão do Instalador de dispositivos StorageGRID no dispositivo de substituição corresponde à versão de software do seu sistema StorageGRID, conforme descrito em instalação e manutenção de hardware para verificar e atualizar a versão do Instalador de dispositivos StorageGRID.
 - [Aparelhos de serviços SG100 e SG1000](#)
 - [SG5600 dispositivos de armazenamento](#)
 - [SG5700 dispositivos de armazenamento](#)
 - [SG6000 dispositivos de armazenamento](#)
- Se você estiver recuperando um nó de grade diferente do nó Admin principal, há conectividade entre o nó de grade sendo recuperado e o nó Admin principal.

Ordem de recuperação de nó se um servidor que hospeda mais de um nó de grade falhar

Se um servidor que hospeda mais de um nó de grade falhar, você poderá recuperar os nós em qualquer ordem. No entanto, se o servidor com falha estiver hospedando o nó Admin principal, você deve recuperar esse nó primeiro. A recuperação do nó de administração principal primeiro impede que outras recuperações de nós parem à medida que esperam para entrar em Contato com o nó de administração principal.

Endereços IP para nós recuperados

Não tente recuperar um nó usando um endereço IP que está atualmente atribuído a qualquer outro nó. Quando você implantar o novo nó, use o endereço IP atual do nó com falha ou um endereço IP não utilizado.

Se você usar um novo endereço IP para implantar o novo nó e, em seguida, recuperar o nó, o novo endereço IP continuará a ser usado para o nó recuperado. Se você quiser reverter para o endereço IP original, use a ferramenta alterar IP após a conclusão da recuperação.

Reúna os materiais necessários para a recuperação do nó da grade

Antes de executar os procedimentos de manutenção, você deve garantir que você tenha os materiais necessários para recuperar um nó de grade com falha.

Item	Notas
Arquivo de instalação do StorageGRID	<p>Se você precisa recuperar um nó de grade, você precisa Transfira os arquivos de instalação do StorageGRID fazer isso para sua plataforma.</p> <p>Observação: você não precisa baixar arquivos se estiver recuperando volumes de armazenamento com falha em um nó de armazenamento.</p>
Serviço de laptop	<p>O computador portátil de serviço tem de ter o seguinte:</p> <ul style="list-style-type: none">• Porta de rede• Cliente SSH (por exemplo, PuTTY)• Navegador da Web suportado

Item	Notas
Arquivo do pacote de recuperação .zip	<p>Obtenha uma cópia do arquivo mais recente do Pacote de recuperação .zip: <code>sgws-recovery-package-id-revision.zip</code></p> <p>O conteúdo do .zip arquivo é atualizado sempre que o sistema é modificado. Você é direcionado para armazenar a versão mais recente do Pacote de recuperação em um local seguro depois de fazer tais alterações. Use a cópia mais recente para recuperar de falhas na grade.</p> <p>Se o nó Admin principal estiver operando normalmente, você poderá fazer o download do Pacote de recuperação do Gerenciador de Grade. Selecione MANUTENÇÃO sistema Pacote de recuperação.</p> <p>Se você não puder acessar o Gerenciador de Grade, poderá encontrar cópias criptografadas do Pacote de recuperação em alguns nós de armazenamento que contêm o serviço ADC. Em cada nó de armazenamento, examine este local para o pacote de recuperação: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Use o pacote de recuperação com o número de revisão mais alto.</p>
Passwords.txt arquivo	Contém as senhas necessárias para acessar os nós de grade na linha de comando. Incluído no Pacote de recuperação.
Frase-passe do provisionamento	A frase-passe é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no Passwords.txt arquivo.
Documentação atual para a sua plataforma	<p>Vá para o site do fornecedor da plataforma para obter documentação.</p> <p>Para obter as versões suportadas atuais da sua plataforma, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".</p>

Baixe e extraia arquivos de instalação do StorageGRID

Baixe o software e extraia os arquivos, a menos que você seja [Recuperando volumes de storage com falha em um nó de storage](#).

Você deve usar a versão do StorageGRID que está atualmente em execução na grade.

Passos

1. Determine qual versão do software está instalada atualmente. Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **sobre**.
2. Vá para "[Página de downloads do NetApp para StorageGRID](#)".
3. Selecione a versão do StorageGRID que está atualmente em execução na grade.

As versões do software StorageGRID têm este formato: 11.x.y.

4. Inicie sessão com o nome de utilizador e a palavra-passe da sua conta NetApp.

5. Leia o Contrato de Licença de Usuário final, marque a caixa de seleção e selecione **aceitar e continuar**.
6. Na coluna **Instalar StorageGRID** da página de download, selecione o `.tgz` arquivo ou `.zip` para sua plataforma.

A versão apresentada no ficheiro de arquivo de instalação tem de corresponder à versão do software atualmente instalado.

Use o `.zip` arquivo se estiver executando o Windows.

Plataforma	Arquivo de instalação
Red Hat Enterprise Linux ou CentOS	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz
Ubuntu ou Debian ou appliances	StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .tgz
VMware	StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .tgz

7. Transfira e extraia o ficheiro de arquivo.
8. Siga o passo apropriado para sua plataforma escolher os arquivos que você precisa, com base em sua plataforma e quais nós de grade você precisa recuperar.

Os caminhos listados na etapa para cada plataforma são relativos ao diretório de nível superior instalado pelo arquivo de arquivo.

9. Se estiver a recuperar um [Red Hat Enterprise Linux ou sistema CentOS](#), selecione os ficheiros apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID em seus hosts RHEL ou CentOS.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL ou CentOS.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.

Caminho e nome do arquivo	Descrição
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Exemplo de função do Ansible e manual de estratégia para configurar hosts RHEL ou CentOS para implantação de contêineres do StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Esquemas de API para StorageGRID. Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.

1. Se estiver a recuperar um [Sistema Ubuntu ou Debian](#), selecione os ficheiros apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Um arquivo de licença do NetApp que não é de produção que pode ser usado para testes e implantações de prova de conceito.
	Pacote DEB para instalar as imagens do nó StorageGRID em hosts Ubuntu ou Debian.
	MD5 checksum para o arquivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .

Caminho e nome do arquivo	Descrição
	Pacote DEB para instalar o serviço host StorageGRID em hosts Ubuntu ou Debian.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Exemplo Ansible role e playbook para configurar hosts Ubuntu ou Debian para a implantação de contentores StorageGRID. Você pode personalizar a função ou o manual de estratégia conforme necessário.
	Esquemas de API para StorageGRID. Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.

1. Se estiver a recuperar um [Sistema VMware](#), selecione os ficheiros apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID.
	Uma licença gratuita que não fornece qualquer direito de suporte para o produto.

Caminho e nome do arquivo	Descrição
	O arquivo de disco da máquina virtual que é usado como um modelo para criar máquinas virtuais de nó de grade.
	O arquivo de modelo Open Virtualization Format (.ovf) e o arquivo de manifesto (.mf) para implantar o nó de administração principal.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de administração não primários.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de arquivamento.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós do Gateway.
	O arquivo de (.ovf`modelo) e o arquivo de manifesto (.mf) para implantar nós de storage baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um exemplo de arquivo de configuração para uso com o <code>deploy-vmware-ovftool.sh</code> script.
	Um script Python usado para automatizar a configuração de um sistema StorageGRID.
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID.
	Um exemplo de script Python que você pode usar para fazer login na API de Gerenciamento de Grade quando o logon único estiver ativado.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> script.

Caminho e nome do arquivo	Descrição
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> script.
	Esquemas de API para StorageGRID. Nota: Antes de executar uma atualização, você pode usar esses esquemas para confirmar que qualquer código que você tenha escrito para usar APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID se você não tiver um ambiente StorageGRID que não seja de produção para teste de compatibilidade de atualização.

1. Se estiver a recuperar um sistema baseado no StorageGRID Appliance, selecione os ficheiros apropriados.

Caminho e nome do arquivo	Descrição
	DEB pacote para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação do pacote de instalação DEB usado pelo instalador do dispositivo StorageGRID para validar se o pacote está intacto após o upload.



Para a instalação do dispositivo, esses arquivos só são necessários se você precisar evitar o tráfego de rede. O dispositivo pode baixar os arquivos necessários do nó de administração principal.

Selecione o procedimento de recuperação do nó

Você deve selecionar o procedimento de recuperação correto para o tipo de nó que falhou.

Nó de grade	Procedimento de recuperação
Mais de um nó de storage	Entre em Contato com o suporte técnico. Se mais de um nó de storage falhar, o suporte técnico deve ajudar na recuperação para evitar inconsistências no banco de dados que podem levar à perda de dados. Um procedimento de recuperação de local pode ser necessário. Como a recuperação do local é realizada pelo suporte técnico
Um único nó de storage	O procedimento de recuperação do nó de armazenamento depende do tipo e duração da falha. Recuperar de falhas no nó de storage

Nó de grade	Procedimento de recuperação
Nó de administração	O procedimento Admin Node depende se você precisa recuperar o nó Admin primário ou um nó Admin não primário. Recuperar de falhas no Admin Node
Nó de gateway	Recuperação de falhas do Gateway Node.
Nó de arquivo	Recuperação de falhas do nó de arquivo.



Se um servidor que hospeda mais de um nó de grade falhar, você poderá recuperar os nós em qualquer ordem. No entanto, se o servidor com falha estiver hospedando o nó Admin principal, você deve recuperar esse nó primeiro. A recuperação do nó de administração principal primeiro impede que outras recuperações de nós parem à medida que esperam para entrar em Contato com o nó de administração principal.

Recuperar de falhas no nó de storage

O procedimento para recuperar um nó de storage com falha depende do tipo de falha e do tipo de nó de storage que falhou.

Use esta tabela para selecionar o procedimento de recuperação para um nó de armazenamento com falha.

Problema	Ação	Notas
<ul style="list-style-type: none"> • Mais de um nó de storage falhou. • Um segundo nó de storage falhou menos de 15 dias após uma falha ou recuperação do nó de storage. <p>Isso inclui o caso em que um nó de storage falha enquanto a recuperação de outro nó de storage ainda está em andamento.</p>	<p>Você deve entrar em Contato com o suporte técnico.</p>	<p>Se todos os nós de storage com falha estiverem no mesmo local, talvez seja necessário executar um procedimento de recuperação de local.</p> <p>O suporte técnico avaliará sua situação e desenvolverá um plano de recuperação.</p> <p>Como a recuperação do local é realizada pelo suporte técnico</p> <p>A recuperação de mais de um nó de storage (ou mais de um nó de storage em 15 dias) pode afetar a integridade do banco de dados Cassandra, o que pode causar perda de dados.</p> <p>O suporte técnico pode determinar quando é seguro iniciar a recuperação de um segundo nó de armazenamento.</p> <p>Nota: Se mais de um nó de armazenamento que contém o serviço ADC falhar em um site, você perderá quaisquer solicitações de serviço de plataforma pendentes para esse site.</p>
<p>Um nó de armazenamento está offline há mais de 15 dias.</p>	<p>Recupere o nó de storage abaixo mais de 15 dias</p>	<p>Este procedimento é necessário para garantir a integridade do banco de dados Cassandra.</p>
<p>Um nó de storage de dispositivo falhou.</p>	<p>Recupere o nó de storage do dispositivo</p>	<p>O procedimento de recuperação para nós de storage do dispositivo é o mesmo para todas as falhas.</p>
<p>Um ou mais volumes de armazenamento falharam, mas a unidade do sistema está intacta</p>	<p>Recuperar de uma falha no volume de armazenamento em que a unidade do sistema está intacta</p>	<p>Este procedimento é usado para nós de storage baseados em software.</p>
<p>A unidade do sistema falhou.</p>	<p>Recuperar de falha na unidade do sistema</p>	<p>O procedimento de substituição do nó depende da plataforma de implantação e se algum volume de storage também falhou.</p>



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

Recupere o nó de storage abaixo mais de 15 dias

Se um nó de storage único estiver offline e não estiver conectado a outros nós de storage por mais de 15 dias, você deverá reconstruir o Cassandra no nó.

O que você vai precisar

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Decommission.**)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Expansion.**)

Sobre esta tarefa

Os nós de storage têm um banco de dados Cassandra que inclui metadados de objetos. Se um nó de storage não conseguir se comunicar com outros nós de storage por mais de 15 dias, o StorageGRID presume que o banco de dados Cassandra do nó está obsoleto. O nó de storage não pode reingressar na grade até que o Cassandra tenha sido reconstruído usando informações de outros nós de storage.

Use este procedimento para reconstruir o Cassandra somente se um nó de armazenamento único estiver inativo. Entre em Contato com o suporte técnico se nós de armazenamento adicionais estiverem offline ou se o Cassandra tiver sido reconstruído em outro nó de armazenamento nos últimos 15 dias; por exemplo, o Cassandra pode ter sido reconstruído como parte dos procedimentos para recuperar volumes de armazenamento com falha ou para recuperar um nó de armazenamento com falha.



Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

Como a recuperação do local é realizada pelo suporte técnico

Passos

1. Se necessário, ligue o nó de armazenamento que precisa ser recuperado.
2. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver logado como root, o prompt muda de `$` para `#`



Se você não conseguir fazer login no nó da grade, o disco do sistema pode não estar intacto. Vá para o procedimento para [recuperando-se da falha da unidade do sistema](#).

1. Execute as seguintes verificações no nó de storage:

a. Emita este comando: `nodetool status`

A saída deve ser de `Connection refused`

b. No Gerenciador de Grade, selecione **support Tools Grid topology**.

c. Selecione **Site nó de armazenamento SSM Serviços**. Verifique se o serviço Cassandra exibe `Not Running`.

d. Selecione **nó de armazenamento SSM recursos**. Verifique se não há status de erro na seção volumes.

e. Emita este comando: `grep -i Cassandra /var/local/log/servermanager.log`

Você deve ver a seguinte mensagem na saída:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. Emita este comando e monitore a saída do script: `check-cassandra-rebuild`

- Se os serviços de armazenamento estiverem em execução, ser-lhe-á pedido que os pare. Digite: **Y**
- Reveja os avisos no script. Se nenhum deles se aplicar, confirme que você deseja reconstruir o Cassandra. Digite: **Y**



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

3. Após a conclusão da reconstrução, execute as seguintes verificações:

a. No Gerenciador de Grade, selecione **support Tools Grid topology**.

b. Selecione **Site nó de armazenamento recuperado SSM Serviços**.

c. Confirme se todos os serviços estão em execução.

d. Selecione **DDS Data Store**.

e. Confirme que o **Status do armazenamento de dados** é `"Up"` e que o **Data Store State** é `"normal."`

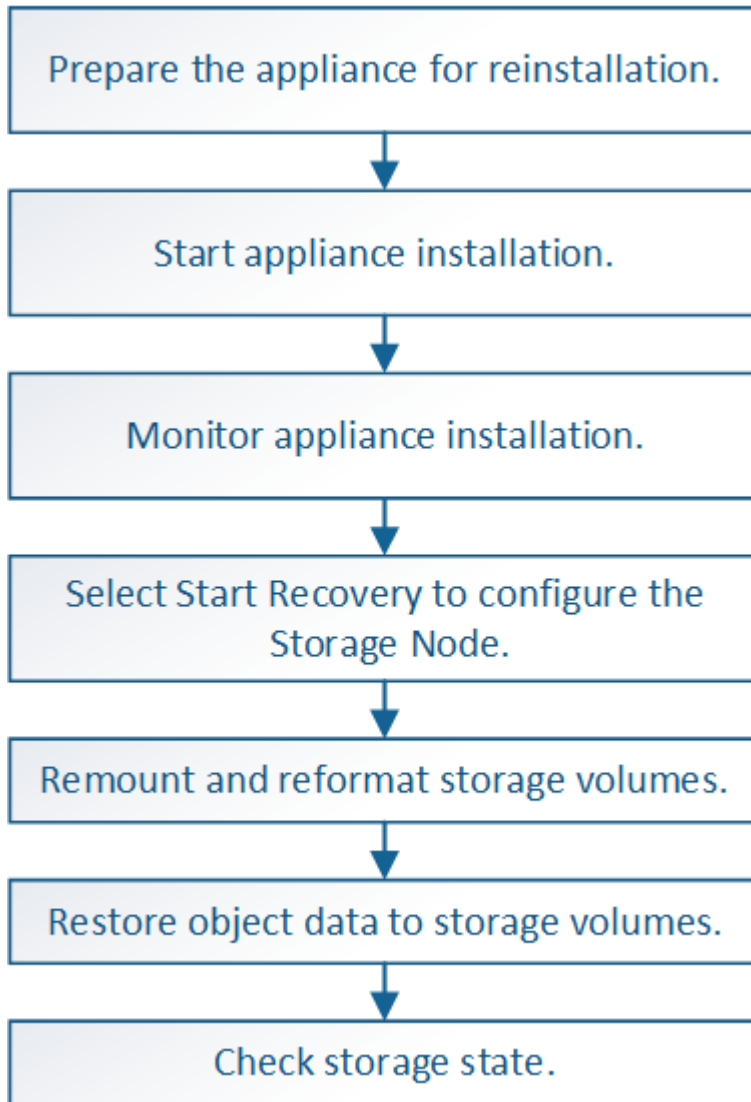
Recupere o nó de storage do dispositivo

O procedimento para recuperar um nó de storage de dispositivo StorageGRID com falha

é o mesmo se você está se recuperando da perda da unidade do sistema ou da perda de volumes de storage somente.

Sobre esta tarefa

Você deve preparar o dispositivo e reinstalar o software, configurar o nó para reingressar na grade, reformatar o armazenamento e restaurar os dados do objeto.



Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.



Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

[Como a recuperação do local é realizada pelo suporte técnico](#)



Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.



Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.



Para procedimentos de manutenção de hardware, como instruções para substituir um controlador ou reinstalar o SANtricity os, consulte as instruções de instalação e manutenção do seu dispositivo de armazenamento.

Informações relacionadas

[Monitorar e solucionar problemas](#)

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG5600 dispositivos de armazenamento](#)

Prepare o nó de storage do dispositivo para reinstalação

Ao recuperar um nó de storage do dispositivo, primeiro você deve preparar o dispositivo para a reinstalação do software StorageGRID.

1. Faça login no nó de storage com falha:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Prepare o nó de storage do dispositivo para a instalação do software StorageGRID. `sgareinstall`
3. Quando solicitado a continuar, digite: `y`

O aparelho reinicializa e sua sessão SSH termina. Normalmente, demora cerca de 5 minutos para que o Instalador de dispositivos StorageGRID fique disponível, embora em alguns casos você possa precisar esperar até 30 minutos.

O nó de armazenamento do dispositivo StorageGRID é redefinido e os dados no nó de armazenamento não estão mais acessíveis. Os endereços IP configurados durante o processo de instalação original devem permanecer intactos; no entanto, é recomendável que você confirme isso quando o procedimento for concluído.

Depois de executar o `sgareinstall` comando, todas as contas, senhas e chaves SSH provisionadas pelo StorageGRID são removidas e novas chaves de host são geradas.

Inicie a instalação do dispositivo StorageGRID

Para instalar o StorageGRID em um nó de armazenamento de dispositivos, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo.

O que você vai precisar

- O dispositivo foi instalado em um rack, conectado às redes e ligado.
- Os links de rede e endereços IP foram configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Você sabe o endereço IP do nó de administrador principal para a grade StorageGRID.
- Todas as sub-redes de rede listadas na página Configuração IP do Instalador de dispositivos StorageGRID foram definidas na Lista de sub-redes de rede de Grade no nó de administração principal.
- Concluiu estas tarefas de pré-requisito seguindo as instruções de instalação e manutenção do seu dispositivo de armazenamento:
 - [SG5600 dispositivos de armazenamento](#)
 - [SG5700 dispositivos de armazenamento](#)
 - [SG6000 dispositivos de armazenamento](#)
- Você está usando um [navegador da web suportado](#).
- Você conhece um dos endereços IP atribuídos ao controlador de computação no dispositivo. Você pode usar o endereço IP da rede Admin (porta de gerenciamento 1 no controlador), da rede de Grade ou da rede do cliente.

Sobre esta tarefa

Para instalar o StorageGRID em um nó de storage do dispositivo:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.
- No decorrer do processo, a instalação é interrompida. Para retomar a instalação, você deve entrar no Gerenciador de Grade e configurar o nó de armazenamento pendente como um substituto para o nó com falha.
- Depois de configurar o nó, o processo de instalação do appliance é concluído e o appliance é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação no dispositivo.

```
https://Controller_IP:8443
```

A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Na seção conexão nó de administrador principal, determine se você precisa especificar o endereço IP do nó de administrador principal.

O Instalador do StorageGRID Appliance pode descobrir esse endereço IP automaticamente, assumindo que o nó de administrador principal, ou pelo menos um outro nó de grade com ADMIN_IP configurado, está presente na mesma sub-rede.

3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Passos
Entrada de IP manual	<ul style="list-style-type: none"> a. Desmarque a caixa de seleção Ativar descoberta de nó de administrador. b. Introduza o endereço IP manualmente. c. Clique em Salvar. d. Aguarde enquanto o estado de conexão para o novo endereço IP se torna "pronto".
Detecção automática de todos os nós de administração principal conectados	<ul style="list-style-type: none"> a. Marque a caixa de seleção Enable Admin Node Discovery (Ativar descoberta de nó de administrador). b. Na lista de endereços IP descobertos, selecione o nó de administração principal para a grade em que este nó de armazenamento do dispositivo será implantado. c. Clique em Salvar. d. Aguarde enquanto o estado de conexão para o novo endereço IP se torna "pronto".

4. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.
5. Na seção Instalação, confirme se o estado atual é ""Pronto para iniciar a instalação do nome do nó na grade com Admin Node admin_ip principal"" e que o botão **Start Installation** está ativado.

Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

6. Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node
discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.



Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG5600 dispositivos de armazenamento](#)

Monitore a instalação do dispositivo StorageGRID

O Instalador de dispositivos StorageGRID fornece o status até que a instalação esteja concluída. Quando a instalação do software estiver concluída, o dispositivo é reinicializado.

1. Para monitorar o progresso da instalação, clique em **Monitor Installation** na barra de menus.

A página Instalação do monitor mostra o progresso da instalação.

Monitor Installation

1. Configure storage		Running
Step	Progress	Status
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Configure volumes	<div style="width: 30%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-00
Configure host settings	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

A barra de status azul indica qual tarefa está atualmente em andamento. As barras de estado verdes indicam tarefas concluídas com êxito.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver reexecutando uma instalação, todas as tarefas que não precisam ser executadas novamente serão mostradas com uma barra de status verde e um status de "concluído".

2. Reveja o progresso das duas primeiras fases de instalação.

- **1. Configurar armazenamento**

Durante essa etapa, o instalador se conecta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o software SANtricity para configurar volumes e configura as configurações do host.

- **2. Instale o os**

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Install StorageGRID** pare e uma mensagem seja exibida no console incorporado solicitando que você aprove esse nó no nó Admin usando o Gerenciador de Grade.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Vá para o procedimento para configurar o nó de armazenamento do dispositivo.

Selecione Iniciar recuperação para configurar o nó de armazenamento do dispositivo

Você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar um nó de armazenamento de appliance como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.

- Você precisa ter implantado um nó de storage do dispositivo de recuperação.
- Você deve saber a data de início de quaisquer trabalhos de reparo para dados codificados por apagamento.
- Você deve ter verificado se o nó de storage não foi reconstruído nos últimos 15 dias.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE Tasks Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).

Quando o nó da grade atingir o estágio "aguardando etapas manuais", vá para o próximo tópico e execute as etapas manuais para remontar e reformatar os volumes de armazenamento do dispositivo.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT	<div style="width: 50%;"></div>	Waiting For Manual Steps

Reset



A qualquer momento durante a recuperação, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó.

Remontagem e formatação dos volumes de storage do dispositivo ("etapas manuais")

É necessário executar manualmente dois scripts para remontar volumes de storage preservados e reformatar os volumes de storage com falha. O primeiro script remonta volumes que são formatados corretamente como volumes de armazenamento StorageGRID. O segundo script reformata quaisquer volumes não montados, reconstrói o banco de dados Cassandra, se necessário, e inicia os serviços.

O que você vai precisar

- Você já substituiu o hardware para quaisquer volumes de armazenamento com falha que você sabe que precisam ser substituídos.

A execução `sn-remount-volumes` do script pode ajudá-lo a identificar volumes de armazenamento com falha adicionais.

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Decommission**.)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Expansion**.)



Contacte o suporte técnico se mais de um nó de armazenamento estiver offline ou se um nó de armazenamento nesta grelha tiver sido reconstruído nos últimos 15 dias. Não execute o `sn-recovery-postinstall.sh` script. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias um do outro pode resultar na perda de dados.

Sobre esta tarefa

Para concluir este procedimento, execute estas tarefas de alto nível:

- Faça login no nó de armazenamento recuperado.

- Execute `sn-remount-volumes` o script para remontar volumes de armazenamento devidamente formatados. Quando este script é executado, ele faz o seguinte:
 - Monta e desmonta cada volume de armazenamento para reproduzir o diário XFS.
 - Executa uma verificação de consistência de arquivo XFS.
 - Se o sistema de arquivos for consistente, determina se o volume de armazenamento é um volume de armazenamento StorageGRID formatado corretamente.
 - Se o volume de armazenamento estiver formatado corretamente, remonta o volume de armazenamento. Todos os dados existentes no volume permanecem intactos.
- Revise a saída do script e resolva quaisquer problemas.
- Execute `sn-recovery-postinstall.sh` o script. Quando este script é executado, ele faz o seguinte.



Não reinicie um nó de armazenamento durante a recuperação antes de ser executado `sn-recovery-postinstall.sh` (etapa 4) para reformatar os volumes de armazenamento com falha e restaurar os metadados de objetos. A reinicialização do nó de armazenamento antes `sn-recovery-postinstall.sh` da conclusão causa erros para serviços que tentam iniciar e faz com que os nós do dispositivo StorageGRID saiam do modo de manutenção.

- Reformata todos os volumes de armazenamento que o `sn-remount-volumes` script não pôde montar ou que foram encontrados para serem formatados incorretamente.



Se um volume de armazenamento for reformatado, todos os dados nesse volume serão perdidos. Você deve executar um procedimento adicional para restaurar dados de objetos de outros locais na grade, assumindo que as regras ILM foram configuradas para armazenar mais de uma cópia de objeto.

- Reconstrói o banco de dados Cassandra no nó, se necessário.
- Inicia os serviços no nó de storage.

Passos

1. Faça login no nó de storage recuperado:

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

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

2. Execute o primeiro script para remontar quaisquer volumes de armazenamento devidamente formatados.



Se todos os volumes de armazenamento forem novos e precisarem ser formatados, ou se todos os volumes de armazenamento tiverem falhado, você poderá pular esta etapa e executar o segundo script para reformatar todos os volumes de armazenamento não montados.

- Execute o script: `sn-remount-volumes`

Esse script pode levar horas para ser executado em volumes de armazenamento que contêm dados.

b. À medida que o script é executado, revise a saída e responda a quaisquer prompts.



Conforme necessário, você pode usar o `tail -f` comando para monitorar o conteúdo do arquivo de log do script (`/var/local/log/sn-remount-volumes.log`). O arquivo de log contém informações mais detalhadas do que a saída da linha de comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sdd =====
Mount and unmount device /dev/sdd and checking file system
```

```

consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

```

Na saída de exemplo, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento tiveram erros.

- /dev/sdb Passou a verificação de consistência do sistema de arquivos XFS e teve uma estrutura de volume válida, então foi remontada com sucesso. Os dados em dispositivos que são remontados pelo script são preservados.
- /dev/sdc Falha na verificação de consistência do sistema de arquivos XFS porque o volume de armazenamento era novo ou corrompido.
- /dev/sdd não foi possível montar porque o disco não foi inicializado ou o superbloco do disco estava corrompido. Quando o script não consegue montar um volume de armazenamento, ele

pergunta se você deseja executar a verificação de consistência do sistema de arquivos.

- Se o volume de armazenamento estiver conectado a um novo disco, responda **N** ao prompt. Você não precisa verificar o sistema de arquivos em um novo disco.
- Se o volume de armazenamento estiver conectado a um disco existente, responda **Y** ao prompt. Você pode usar os resultados da verificação do sistema de arquivos para determinar a origem da corrupção. Os resultados são guardados no `/var/local/log/sn-remount-volumes.log` ficheiro de registo.
- `/dev/sde` Passou a verificação de consistência do sistema de ficheiros XFS e tinha uma estrutura de volume válida; no entanto, a ID do nó LDR no `volID` ficheiro não correspondia à ID deste nó de armazenamento (a `configured LDR noID` apresentada na parte superior). Esta mensagem indica que este volume pertence a outro nó de armazenamento.

3. Revise a saída do script e resolva quaisquer problemas.



Se um volume de armazenamento falhou na verificação de consistência do sistema de arquivos XFS ou não pôde ser montado, revise cuidadosamente as mensagens de erro na saída. Você deve entender as implicações da execução `sn-recovery-postinstall.sh` do script nesses volumes.

- Verifique se os resultados incluem uma entrada para todos os volumes esperados. Se algum volume não estiver listado, execute novamente o script.
- Reveja as mensagens de todos os dispositivos montados. Certifique-se de que não existem erros que indiquem que um volume de armazenamento não pertence a este nó de armazenamento.

No exemplo, a saída para `/dev/sde` inclui a seguinte mensagem de erro:

```
Error: This volume does not belong to this node. Fix the attached volume and re-run this script.
```



Se um volume de armazenamento for comunicado como pertencente a outro nó de armazenamento, contacte o suporte técnico. Se você executar `sn-recovery-postinstall.sh` o script, o volume de armazenamento será reformatado, o que pode causar perda de dados.

- Se não for possível montar qualquer dispositivo de armazenamento, anote o nome do dispositivo e repare ou substitua o dispositivo.



Deve reparar ou substituir quaisquer dispositivos de armazenamento que não possam ser montados.

Você usará o nome do dispositivo para procurar o ID do volume, que é a entrada necessária quando você executar `repair-data` o script para restaurar os dados do objeto para o volume (o próximo procedimento).

- Depois de reparar ou substituir todos os dispositivos não montáveis, execute o `sn-remount-volumes` script novamente para confirmar que todos os volumes de armazenamento que podem ser remontados foram remontados.



Se um volume de armazenamento não puder ser montado ou for formatado incorretamente e você continuar para a próxima etapa, o volume e quaisquer dados no volume serão excluídos. Se você tiver duas cópias de dados de objeto, você terá apenas uma única cópia até concluir o próximo procedimento (restaurando dados de objeto).



Não execute `sn-recovery-postinstall.sh` o script se você acredita que os dados restantes em um volume de armazenamento com falha não podem ser reconstruídos de outro lugar na grade (por exemplo, se sua política de ILM usar uma regra que faça apenas uma cópia ou se os volumes tiverem falhado em vários nós). Em vez disso, entre em Contato com o suporte técnico para determinar como recuperar seus dados.

4. Execute `sn-recovery-postinstall.sh` o script: `sn-recovery-postinstall.sh`

Este script reformata quaisquer volumes de armazenamento que não puderam ser montados ou que foram encontrados para serem formatados incorretamente; reconstrói o banco de dados Cassandra no nó, se necessário; e inicia os serviços no nó Storage Node.

Tenha em atenção o seguinte:

- O script pode levar horas para ser executado.
- Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
- Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
- O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar a sessão SSH, mas você pode visualizar o progresso da página recuperação.
- Se o nó de armazenamento usar o serviço RSM, o script pode parecer parar por 5 minutos à medida que os serviços do nó são reiniciados. Este atraso de 5 minutos é esperado sempre que o serviço RSM arranca pela primeira vez.



O serviço RSM está presente nos nós de storage que incluem o serviço ADC.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. À medida que o `sn-recovery-postinstall.sh` script é executado, monitore a página recuperação no Gerenciador de Grade.

A barra de progresso e a coluna Estágio na página recuperação fornecem um status de alto nível `sn-recovery-postinstall.sh` do script.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
No results found.			

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT	<div style="width: 50%; background-color: #0070C0;"></div>	Recovering Cassandra

Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para quaisquer volumes de armazenamento que foram formatados pelo script, conforme descrito no procedimento seguinte.

Informações relacionadas


[Reveja os avisos de recuperação da unidade do sistema Storage Node](#)

[Restaure os dados de objeto para o volume de storage do dispositivo](#)

Restaure os dados de objeto para o volume de storage do dispositivo

Depois de recuperar volumes de armazenamento para o nó de armazenamento do dispositivo, você pode restaurar os dados do objeto que foram perdidos quando o nó de armazenamento falhou.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected**  na guia **NODES > Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.
- Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. A restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage devido à

latência associada a recuperações de sistemas de armazenamento de arquivamento externos.

Sobre o `repair-data` script

Para restaurar os dados do objeto, execute o `repair-data` script. Este script inicia o processo de restauração de dados de objeto e trabalha com a digitalização ILM para garantir que as regras ILM sejam atendidas.

Selecione **dados replicados** ou **dados codificados por apagamento (EC)** abaixo para aprender as diferentes opções para o `repair-data` script, com base se você está restaurando dados replicados ou dados codificados por apagamento. Se você precisar restaurar ambos os tipos de dados, deverá executar ambos os conjuntos de comandos.



Para obter mais informações sobre o `repair-data` script, insira `repair-data --help` a partir da linha de comando do nó Admin principal.

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA) e período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados por apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```



O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Encontre o nome do host para nó de armazenamento

1. Faça login no nó de administração principal:

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

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

2. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte `cat /etc/hosts:`.

Repare os dados se todos os volumes tiverem falhado

Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se apenas alguns volumes tiverem falhado, vá para [Repare os dados se apenas alguns volumes tiverem falhado](#).



Não é possível executar `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em Contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. [Monitorar e solucionar problemas](#)Consulte

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de storage.

Este comando repara os dados codificados por apagamento em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Repare os dados se apenas alguns volumes tiverem falhado

Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se todos os volumes tiverem falhado, vá para [Repare os dados se todos os volumes tiverem falhado](#).

Introduza as IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estão em uma sequência.

Todos os volumes devem estar no mesmo nó de storage. Se precisar restaurar volumes para mais de um nó de storage, entre em Contato com o suporte técnico.

Dados replicados

Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes 0001, 0005 e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura os dados codificados por apagamento para o volume 0007 em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por apagamento para todos os volumes no intervalo 0004 para 0006 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em uma sequência: Este comando restaura dados codificados por apagamento para volumes 000A, 000C e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

A `repair-data` operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Monitorize as reparações

Monitore o status dos trabalhos de reparo, com base se você usa **dados replicados**, **dados codificados por apagamento (EC)** ou ambos.

Dados replicados

- Para determinar se as reparações estão concluídas:
 - a. Selecione **NODES > Storage Node a ser reparado > ILM**.
 - b. Reveja os atributos na seção avaliação. Quando os reparos estiverem concluídos, o atributo **aguardando - All** indica objetos 0D.
- Para monitorizar a reparação em mais detalhes:
 - a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Selecione **Grid > Storage Node a ser reparado > LDR > Data Store**.
 - c. Use uma combinação dos seguintes atributos para determinar, assim como possível, se as reparações replicadas estão concluídas.



As inconsistências do Cassandra podem estar presentes e as reparações falhadas não são rastreadas.

- * Tentativas de reparos (XRPA): **Use este atributo para rastrear o progresso de reparos replicados. Esse atributo aumenta cada vez que um nó de storage tenta reparar um objeto de alto risco. Quando este atributo não aumenta por um período superior ao período de digitalização atual (fornecido pelo atributo *período de digitalização — estimado), significa que a digitalização ILM não encontrou objetos de alto risco que precisam ser reparados em nenhum nó.**



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração ILM.

- **Período de digitalização — estimado (XSCM):** Use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Repairs tented** não aumentar durante um período superior ao período de digitalização atual, é provável que sejam efetuadas reparações replicadas. Note que o período de digitalização pode mudar. O atributo **período de digitalização — estimado (XSCM)** aplica-se a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico de atributos **período de digitalização — estimado** para a grade para determinar um período de tempo apropriado.
- Opcionalmente, para obter uma conclusão percentual estimada para o reparo replicado, adicione a `show-replicated-repair-status` opção ao comando `repair-data`.

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA)** e **período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Para monitorar o reparo de dados codificados por apagamento e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por apagamento:

- Selecione **SUPPORT > Tools > Metrics** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **EC Overview** na seção Grafana. Veja os painéis **Grid EC Job tempo estimado para conclusão** e **Grid EC Job percentage Completed**.

- Use este comando para ver o status de uma operação específica `repair-data`:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilize este comando para listar todas as reparações:

```
repair-data show-ec-repair-status
```

A saída lista informações, `repair ID` incluindo , para todas as reparações anteriores e atualmente em execução.

2. Se a saída mostrar que a operação de reparo falhou, use a `--repair-id` opção para tentar novamente a reparação.

Este comando tenta novamente um reparo de nó com falha, usando a ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado de armazenamento após recuperar o nó de armazenamento do dispositivo

Depois de recuperar um nó de armazenamento de dispositivo, você deve verificar se o estado desejado do nó de armazenamento de dispositivo está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- O nó de armazenamento foi recuperado e a recuperação de dados está concluída.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Verifique os valores de **nó de armazenamento recuperado > LDR > armazenamento > Estado de armazenamento — desejado** e **Estado de armazenamento — atual**.

O valor de ambos os atributos deve ser Online.

3. Se o estado de armazenamento - desejado estiver definido como somente leitura, execute as seguintes etapas:

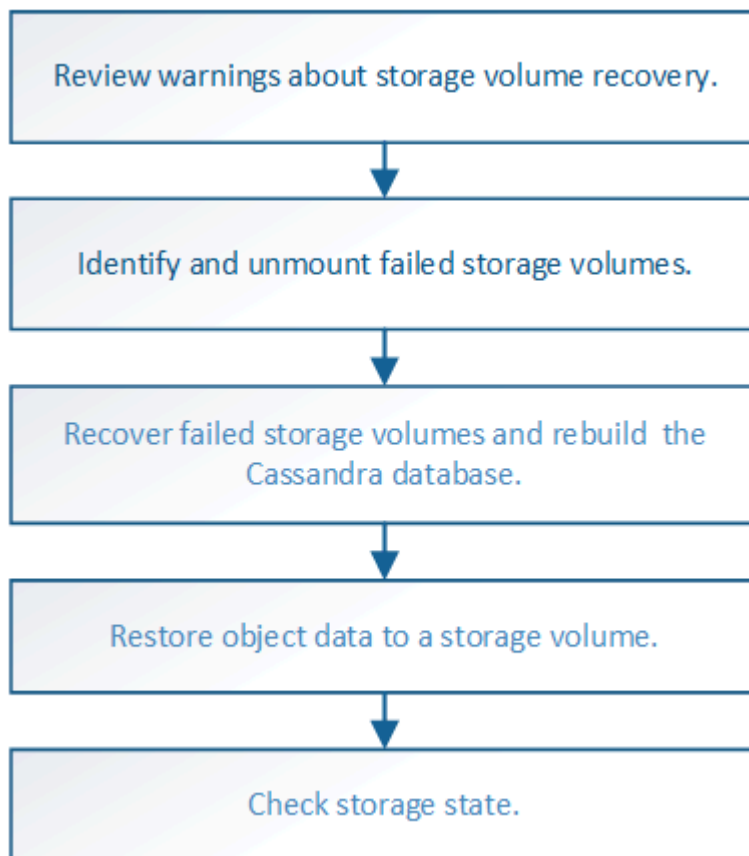
- a. Clique na guia **Configuração**.
- b. Na lista suspensa **Estado de armazenamento - desejado**, selecione **Online**.
- c. Clique em **aplicar alterações**.
- d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — desejado** e **Estado de armazenamento — atual** são atualizados para Online.

Recuperar de uma falha no volume de armazenamento em que a unidade do sistema está intacta

Você deve concluir uma série de tarefas para recuperar um nó de storage baseado em software em que um ou mais volumes de armazenamento no nó de armazenamento falharam, mas a unidade do sistema está intacta. Se apenas os volumes de armazenamento tiverem falhado, o nó de armazenamento ainda estará disponível para o sistema StorageGRID.

Sobre esta tarefa

Este procedimento de recuperação aplica-se apenas a nós de storage baseados em software. Se os volumes de armazenamento tiverem falhado num nó de armazenamento de dispositivo, siga o procedimento para ""Recover Appliance Storage Node"".



Informações relacionadas

[Recupere o nó de storage do dispositivo](#)

Reveja os avisos sobre a recuperação do volume de armazenamento

Antes de recuperar volumes de armazenamento com falha para um nó de

armazenamento, deve rever os seguintes avisos.

Os volumes de armazenamento (ou rangedbs) em um nó de armazenamento são identificados por um número hexadecimal, que é conhecido como ID de volume. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. O primeiro armazenamento de objetos (volume 0) em cada nó de armazenamento usa até 4 TB de espaço para metadados de objetos e operações de banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objeto. Todos os outros volumes de storage são usados exclusivamente para dados de objetos.

Se o volume 0 falhar e precisar ser recuperado, o banco de dados Cassandra pode ser reconstruído como parte do procedimento de recuperação de volume. Cassandra também pode ser reconstruída nas seguintes circunstâncias:

- Um nó de armazenamento é colocado de volta online depois de estar offline por mais de 15 dias.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de storage. Se muitos nós de storage estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. A perda de dados pode ocorrer se o Cassandra for reconstruído quando muitos nós de storage estiverem off-line ou se dois ou mais nós de storage forem reconstruídos em até 15 dias um do outro.



Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.



Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

Como a recuperação do local é realizada pelo suporte técnico



Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.



Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.

Informações relacionadas

[Monitorar e solucionar problemas](#)

[Avisos e considerações para a recuperação do nó da grade](#)

Identificar e desmontar volumes de storage com falha

Ao recuperar um nó de storage com volumes de storage com falha, você deve identificar e desmontar os volumes com falha. Você deve verificar se apenas os volumes de

armazenamento com falha são reformatados como parte do procedimento de recuperação.

O que você vai precisar

Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

Você deve recuperar volumes de armazenamento com falha o mais rápido possível.

A primeira etapa do processo de recuperação é detectar volumes que se desprenderam, precisam ser desmontados ou têm erros de e/S. Se os volumes com falha ainda estiverem anexados, mas tiverem um sistema de arquivos corrompido aleatoriamente, o sistema poderá não detectar qualquer corrupção em partes não utilizadas ou não alocadas do disco.



Você deve concluir este procedimento antes de executar etapas manuais para recuperar os volumes, como adicionar ou reanexar os discos, parar o nó, iniciar o nó ou reinicializar. Caso contrário, quando você executa `reformat_storage_block_devices.rb` o script, você pode encontrar um erro de sistema de arquivos que faz com que o script pendure ou falhe.



Repare o hardware e conecte corretamente os discos antes de executar o `reboot` comando.

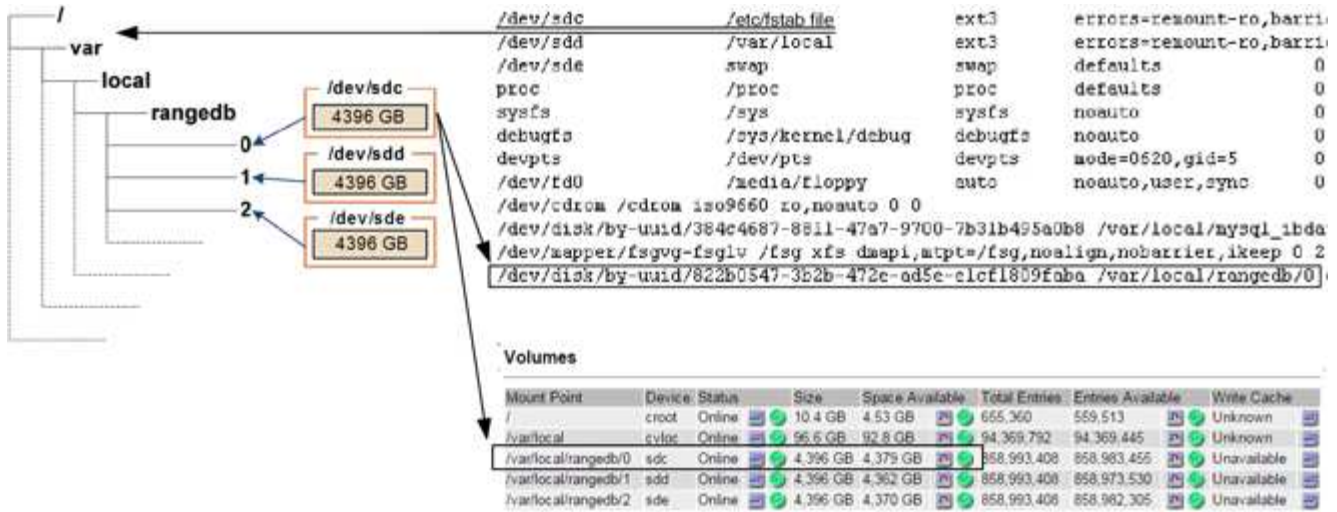


Identifique cuidadosamente os volumes de armazenamento com falha. Você usará essas informações para verificar quais volumes devem ser reformatados. Uma vez que um volume tenha sido reformatado, os dados no volume não podem ser recuperados.

Para recuperar corretamente volumes de armazenamento com falha, você precisa saber os nomes dos dispositivos dos volumes de armazenamento com falha e suas IDs de volume.

Na instalação, cada dispositivo de armazenamento recebe um identificador exclusivo universal (UUID) do sistema de arquivos e é montado em um diretório `rangedb` no nó de armazenamento usando esse UUID do sistema de arquivos atribuído. O sistema de arquivos UUID e o diretório `rangedb` são listados no `/etc/fstab` arquivo. O nome do dispositivo, o diretório `rangedb` e o tamanho do volume montado são exibidos no Gerenciador de Grade.

No exemplo a seguir, o dispositivo `/dev/sdc` tem um tamanho de volume de 4 TB, é montado no `/var/local/rangedb/0`, usando o nome do dispositivo `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` no `/etc/fstab` arquivo:



Passos

- Execute as etapas a seguir para gravar os volumes de armazenamento com falha e os nomes de seus dispositivos:
 - Selecione **SUPPORT > Tools > Grid topology**.
 - Selecione **site nó de armazenamento com falha LDR armazenamento Visão geral Principal** e procure armazenamentos de objetos com alarmes.

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

- Selecione **site nó de armazenamento com falha SSM recursos Visão geral Principal**. Determine o ponto de montagem e o tamanho do volume de cada volume de armazenamento com falha identificado na etapa anterior.

Os armazenamentos de objetos são numerados em notação hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. No exemplo, o armazenamento de objetos com uma ID de 0000 corresponde `/var/local/rangedb/0` com o nome do dispositivo `sdc` e um tamanho de 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	crout	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

- Faça login no nó de storage com falha:

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

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

3. Execute o script a seguir para interromper os serviços de storage e desmontar um volume de storage com falha:

```
sn-unmount-volume object_store_ID
```

O `object_store_ID` é a ID do volume de armazenamento com falha. Por exemplo, especifique `0` no comando para um armazenamento de objetos com ID `0000`.

4. Se solicitado, pressione `y` para interromper os serviços de armazenamento no nó de armazenamento.



Se os serviços de armazenamento já estiverem parados, você não será solicitado. O serviço Cassandra é interrompido apenas para o volume `0`.

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

Em alguns segundos, os serviços de armazenamento são interrompidos e o volume é desmontado. As mensagens são exibidas indicando cada etapa do processo. A mensagem final indica que o volume está desmontado.

Recuperar volumes de armazenamento com falha e reconstruir o banco de dados Cassandra

Você deve executar um script que reformata e remonta o armazenamento em volumes de armazenamento com falha e reconstrói o banco de dados Cassandra no nó de armazenamento se o sistema determinar que é necessário.

- Tem de ter o `Passwords.txt` ficheiro.
- As unidades de sistema no servidor devem estar intactas.
- A causa da falha deve ter sido identificada e, se necessário, o hardware de armazenamento de substituição já deve ter sido adquirido.
- O tamanho total do armazenamento de substituição deve ser o mesmo que o original.

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Decommission.**)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Expansion.**)
- Você [revisou os avisos sobre a recuperação do volume de armazenamento](#)tem .

a. Conforme necessário, substitua o armazenamento físico ou virtual com falha associado aos volumes de armazenamento com falha identificados e desmontados anteriormente.

Depois de substituir o storage, verifique novamente ou reinicialize para ter certeza de que ele é reconhecido pelo sistema operacional, mas não remonte os volumes. O armazenamento é remontado e adicionado em `/etc/fstab` um passo posterior.

b. Faça login no nó de storage com falha:

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

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

c. Use um editor de texto (vi ou vim) para excluir volumes com falha do `/etc/fstab` arquivo e, em seguida, salve o arquivo.



Comentar um volume com falha `/etc/fstab` no arquivo é insuficiente. O volume deve ser excluído `fstab`, pois o processo de recuperação verifica se todas as linhas no `fstab` arquivo correspondem aos sistemas de arquivos montados.

d. Reformate quaisquer volumes de armazenamento com falha e reconstrua o banco de dados Cassandra, se necessário. Introduza: `reformat_storage_block_devices.rb`

- Se os serviços de armazenamento estiverem em execução, ser-lhe-á pedido que os pare. Digite: **Y**
- Você será solicitado a reconstruir o banco de dados do Cassandra, se necessário.
 - Reveja os avisos. Se nenhum deles se aplicar, reconstrua o banco de dados Cassandra. Digite: **Y**
 - Se mais de um nó de armazenamento estiver offline ou se outro nó de armazenamento tiver sido reconstruído nos últimos 15 dias. Digite: **N**

O script sairá sem reconstruir o Cassandra. Entre em Contato com o suporte técnico.

- Para cada unidade `rangedb` no nó de armazenamento, quando for solicitado: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, Insira uma das seguintes respostas:
 - **y** para reformatar uma unidade com erros. Isso reformata o volume de armazenamento e adiciona o volume de armazenamento reformatado ao `/etc/fstab` arquivo.
 - **n** se a unidade não contiver erros e você não quiser reformatá-la.



Selecionar **n** sai do script. Monte a unidade (se você acha que os dados na unidade devem ser retidos e a unidade foi desmontada por erro) ou remova a unidade. Em seguida, execute o `reformat_storage_block_devices.rb` comando novamente.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

Na saída de exemplo a seguir, a unidade `/dev/sdf` deve ser reformatada e o Cassandra não precisa ser reconstruído:


```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done. Now do manual steps to
restore copies of data.
```

Restaure os dados de objetos para o volume de storage em que a unidade do sistema esteja intacta

Depois de recuperar um volume de armazenamento em um nó de armazenamento em que a unidade do sistema está intacta, você pode restaurar os dados do objeto que foram perdidos quando o volume de armazenamento falhou.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected**  na guia **NODES > Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.
- Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. A restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage devido à latência associada a recuperações de sistemas de armazenamento de arquivamento externos.

Sobre o `repair-data` script

Para restaurar os dados do objeto, execute o `repair-data` script. Este script inicia o processo de restauração de dados de objeto e trabalha com a digitalização ILM para garantir que as regras ILM sejam atendidas.

Selecione **dados replicados** ou **dados codificados por apagamento (EC)** abaixo para aprender as diferentes opções para o `repair-data` script, com base se você está restaurando dados replicados ou dados codificados por apagamento. Se você precisar restaurar ambos os tipos de dados, deverá executar ambos os conjuntos de comandos.



Para obter mais informações sobre o `repair-data` script, insira `repair-data --help` a partir da linha de comando do nó Admin principal.

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA) e período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados por apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```



O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Encontre o nome do host para nó de armazenamento

1. Faça login no nó de administração principal:

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

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

2. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte `cat /etc/hosts:`.

Repare os dados se todos os volumes tiverem falhado

Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se apenas alguns volumes tiverem falhado, vá para [Repare os dados se apenas alguns volumes tiverem falhado](#).



Não é possível executar `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em Contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. [Monitorar e solucionar problemas](#) Consulte

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de storage.

Este comando repara os dados codificados por apagamento em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Repare os dados se apenas alguns volumes tiverem falhado

Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se todos os volumes tiverem falhado, vá para [Repare os dados se todos os volumes tiverem falhado](#).

Introduza as IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estão em uma sequência.

Todos os volumes devem estar no mesmo nó de storage. Se precisar restaurar volumes para mais de um nó de storage, entre em Contato com o suporte técnico.

Dados replicados

Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes 0001, 0005 e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura os dados codificados por apagamento para o volume 0007 em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por apagamento para todos os volumes no intervalo 0004 para 0006 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em uma sequência: Este comando restaura dados codificados por apagamento para volumes 000A, 000C e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

A `repair-data` operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Monitorize as reparações

Monitore o status dos trabalhos de reparo, com base se você usa **dados replicados**, **dados codificados por apagamento (EC)** ou ambos.

Dados replicados

- Para determinar se as reparações estão concluídas:
 - a. Selecione **NODES > Storage Node a ser reparado > ILM**.
 - b. Reveja os atributos na seção avaliação. Quando os reparos estiverem concluídos, o atributo **aguardando - All** indica objetos 0D.
- Para monitorizar a reparação em mais detalhes:
 - a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Selecione **Grid > Storage Node a ser reparado > LDR > Data Store**.
 - c. Use uma combinação dos seguintes atributos para determinar, assim como possível, se as reparações replicadas estão concluídas.



As inconsistências do Cassandra podem estar presentes e as reparações falhadas não são rastreadas.

- * Tentativas de reparos (XRPA): **Use este atributo para rastrear o progresso de reparos replicados. Esse atributo aumenta cada vez que um nó de storage tenta reparar um objeto de alto risco. Quando este atributo não aumenta por um período superior ao período de digitalização atual (fornecido pelo atributo *período de digitalização — estimado), significa que a digitalização ILM não encontrou objetos de alto risco que precisam ser reparados em nenhum nó.**



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração ILM.

- **Período de digitalização — estimado (XSCM):** Use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Repairs tented** não aumentar durante um período superior ao período de digitalização atual, é provável que sejam efetuadas reparações replicadas. Note que o período de digitalização pode mudar. O atributo **período de digitalização — estimado (XSCM)** aplica-se a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico de atributos **período de digitalização — estimado** para a grade para determinar um período de tempo apropriado.
- Opcionalmente, para obter uma conclusão percentual estimada para o reparo replicado, adicione a `show-replicated-repair-status` opção ao comando `repair-data`.

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA)** e **período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Para monitorar o reparo de dados codificados por apagamento e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por apagamento:

- Selecione **SUPPORT > Tools > Metrics** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **EC Overview** na seção Grafana. Veja os painéis **Grid EC Job tempo estimado para conclusão** e **Grid EC Job percentage Completed**.

- Use este comando para ver o status de uma operação específica `repair-data`:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilize este comando para listar todas as reparações:

```
repair-data show-ec-repair-status
```

A saída lista informações, `repair ID` incluindo , para todas as reparações anteriores e atualmente em execução.

2. Se a saída mostrar que a operação de reparo falhou, use a `--repair-id` opção para tentar novamente a reparação.

Este comando tenta novamente um reparo de nó com falha, usando a ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado do armazenamento depois de recuperar volumes de armazenamento

Depois de recuperar volumes de armazenamento, você deve verificar se o estado desejado do nó de armazenamento está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- O nó de armazenamento foi recuperado e a recuperação de dados está concluída.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Verifique os valores de **nó de armazenamento recuperado > LDR > armazenamento > Estado de armazenamento — desejado** e **Estado de armazenamento — atual**.

O valor de ambos os atributos deve ser Online.

3. Se o estado de armazenamento - desejado estiver definido como somente leitura, execute as seguintes etapas:
 - a. Clique na guia **Configuração**.

- b. Na lista suspensa **Estado de armazenamento - desejado**, selecione **Online**.
- c. Clique em **aplicar alterações**.
- d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — desejado** e **Estado de armazenamento — atual** são atualizados para Online.

Recuperar de falha na unidade do sistema

Se a unidade do sistema em um nó de storage baseado em software tiver falhado, o nó de storage não estará disponível para o sistema StorageGRID. Você deve concluir um conjunto específico de tarefas para recuperar de uma falha na unidade do sistema.

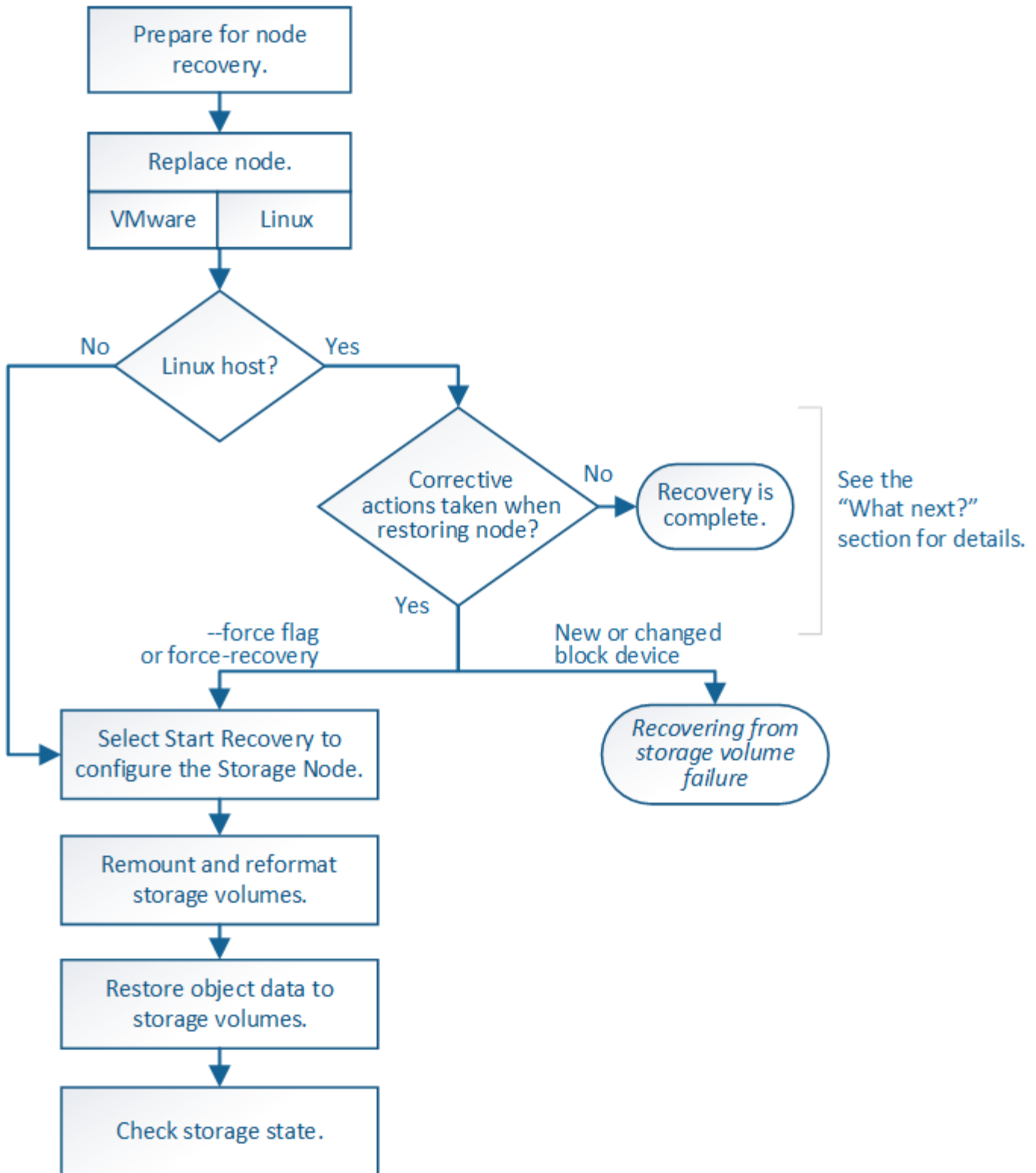
Sobre esta tarefa

Use este procedimento para recuperar de uma falha na unidade do sistema em um nó de armazenamento baseado em software. Este procedimento inclui os passos a seguir se quaisquer volumes de armazenamento também falharem ou não puderem ser remontados.



Este procedimento aplica-se apenas a nós de storage baseados em software. Você deve seguir um procedimento diferente para recuperar um nó de storage do dispositivo.

[Recupere o nó de storage do dispositivo](#)



Reveja os avisos de recuperação da unidade do sistema Storage Node

Antes de recuperar uma unidade de sistema com falha de um nó de armazenamento, deve rever os seguintes avisos.

Os nós de storage têm um banco de dados Cassandra que inclui metadados de objetos. O banco de dados Cassandra pode ser reconstruído nas seguintes circunstâncias:

- Um nó de armazenamento é colocado de volta online depois de estar offline por mais de 15 dias.
- Um volume de armazenamento falhou e foi recuperado.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de storage. Se muitos nós de storage estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. A perda de dados pode ocorrer se o Cassandra for reconstruído quando muitos nós de storage estiverem off-line ou se dois ou mais nós de storage forem reconstruídos em até 15 dias um do outro.



Se mais de um nó de armazenamento tiver falhado (ou estiver offline), contacte o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de storage em menos de 15 dias após uma falha ou recuperação do nó de storage, entre em Contato com o suporte técnico. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias pode resultar na perda de dados.



Se mais de um nó de armazenamento em um local tiver falhado, um procedimento de recuperação do local pode ser necessário. Entre em Contato com o suporte técnico.

Como a recuperação do local é realizada pelo suporte técnico



Se este nó de armazenamento estiver no modo de manutenção somente leitura para permitir a recuperação de objetos por outro nó de armazenamento com volumes de armazenamento com falha, recupere volumes no nó de armazenamento com volumes de armazenamento com falha antes de recuperar este nó de armazenamento com falha. Consulte as instruções para recuperar da perda de volumes de armazenamento em que a unidade do sistema está intacta.



Se as regras ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir num volume de armazenamento que falhou, não será possível recuperar o objeto.



Se você encontrar um alarme Serviços: Status - Cassandra (SVST) durante a recuperação, consulte as instruções de monitoramento e solução de problemas para recuperar do alarme reconstruindo o Cassandra. Após a reconstrução do Cassandra, os alarmes devem ser apagados. Se os alarmes não forem apagados, contacte o suporte técnico.

Informações relacionadas

[Monitorar e solucionar problemas](#)

[Avisos e considerações para a recuperação do nó da grade](#)

[Recuperar de uma falha no volume de armazenamento em que a unidade do sistema está intacta](#)

Substitua o nó de storage

Se a unidade do sistema tiver falhado, tem de substituir primeiro o nó de armazenamento.

Você deve selecionar o procedimento de substituição do nó para sua plataforma. As etapas para substituir um nó são as mesmas para todos os tipos de nós de grade.



Este procedimento aplica-se apenas a nós de storage baseados em software. Você deve seguir um procedimento diferente para recuperar um nó de storage do dispositivo.

Recupere o nó de storage do dispositivo

- Linux:* se você não tiver certeza se a unidade de sistema falhou, siga as instruções para substituir o nó para determinar quais etapas de recuperação são necessárias.

Plataforma	Procedimento
VMware	Substitua um nó VMware
Linux	Substitua um nó Linux
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecione Iniciar recuperação para configurar o nó de armazenamento

Depois de substituir um nó de armazenamento, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.
- Você deve saber a data de início de quaisquer trabalhos de reparo para dados codificados por apagamento.
- Você deve ter verificado se o nó de storage não foi reconstruído nos últimos 15 dias.

Sobre esta tarefa

Se o nó de armazenamento for instalado como um contentor em um host Linux, você deverá executar esta etapa somente se um deles for verdadeiro:

- Você teve que usar o `--force` sinalizador para importar o nó, ou você emitiu `storagegrid node force-recovery node-name`
- Você teve que fazer uma reinstalação completa do nó, ou você precisava restaurar `/var/local`.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE Tasks Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.

4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

i Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó para um estado pré-instalado, da seguinte forma:

- **VMware:** Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a

recuperação, reimplante o nó.

- * Linux*: Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`

6. Quando o nó de armazenamento atingir o estágio "aguardando etapas manuais", vá para a próxima tarefa no procedimento de recuperação para remontar e reformatar os volumes de armazenamento.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT	<div style="width: 100%; height: 10px; background-color: #0070C0;"></div>	Waiting For Manual Steps

Reset

Informações relacionadas

[Prepare o aparelho para reinstalação \(apenas substituição da plataforma\)](#)

Remontagem e reformatação dos volumes de storage ("etapas manuais")

É necessário executar manualmente dois scripts para remontar volumes de storage preservados e reformatar os volumes de storage com falha. O primeiro script remonta volumes que são formatados corretamente como volumes de armazenamento StorageGRID. O segundo script reformata quaisquer volumes não montados, reconstrói Cassandra, se necessário, e inicia serviços.

O que você vai precisar

- Você já substituiu o hardware para quaisquer volumes de armazenamento com falha que você sabe que precisam ser substituídos.

A execução `sn-remount-volumes` do script pode ajudá-lo a identificar volumes de armazenamento com falha adicionais.

- Você verificou que a desativação de um nó de storage não está em andamento ou interrompeu o procedimento de desativação do nó. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Decommission.**)
- Você verificou que uma expansão não está em andamento. (No Gerenciador de Grade, selecione **MAINTENANCE Tasks Expansion.**)
- Você [Revisou os avisos para recuperação da unidade do sistema Storage Node](#)tem .



Contacte o suporte técnico se mais de um nó de armazenamento estiver offline ou se um nó de armazenamento nesta grelha tiver sido reconstruído nos últimos 15 dias. Não execute o `sn-recovery-postinstall.sh` script. A reconstrução do Cassandra em dois ou mais nós de storage em até 15 dias um do outro pode resultar na perda de dados.

Sobre esta tarefa

Para concluir este procedimento, execute estas tarefas de alto nível:

- Faça login no nó de armazenamento recuperado.
- Execute `sn-remount-volumes` o script para remontar volumes de armazenamento devidamente formatados. Quando este script é executado, ele faz o seguinte:
 - Monta e desmonta cada volume de armazenamento para reproduzir o diário XFS.
 - Executa uma verificação de consistência de arquivo XFS.
 - Se o sistema de arquivos for consistente, determina se o volume de armazenamento é um volume de armazenamento StorageGRID formatado corretamente.
 - Se o volume de armazenamento estiver formatado corretamente, remonta o volume de armazenamento. Todos os dados existentes no volume permanecem intactos.
- Revise a saída do script e resolva quaisquer problemas.
- Execute `sn-recovery-postinstall.sh` o script. Quando este script é executado, ele faz o seguinte.



Não reinicie um nó de storage durante a recuperação antes de ser executado `sn-recovery-postinstall.sh` para reformatar os volumes de armazenamento com falha e restaurar os metadados de objetos. A reinicialização do nó de armazenamento antes `sn-recovery-postinstall.sh` da conclusão causa erros para serviços que tentam iniciar e faz com que os nós do dispositivo StorageGRID saiam do modo de manutenção. Consulte a etapa para [script de pós-instalação](#).

- Reformata todos os volumes de armazenamento que o `sn-remount-volumes` script não pôde montar ou que foram encontrados para serem formatados incorretamente.



Se um volume de armazenamento for reformatado, todos os dados nesse volume serão perdidos. Você deve executar um procedimento adicional para restaurar dados de objetos de outros locais na grade, assumindo que as regras ILM foram configuradas para armazenar mais de uma cópia de objeto.

- Reconstrói o banco de dados Cassandra no nó, se necessário.
- Inicia os serviços no nó de storage.

Passos

1. Faça login no nó de storage recuperado:

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

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

2. Execute o primeiro script para remontar quaisquer volumes de armazenamento devidamente formatados.



Se todos os volumes de armazenamento forem novos e precisarem ser formatados, ou se todos os volumes de armazenamento tiverem falhado, você poderá pular esta etapa e executar o segundo script para reformatar todos os volumes de armazenamento não montados.

a. Execute o script: `sn-remount-volumes`

Esse script pode levar horas para ser executado em volumes de armazenamento que contêm dados.

b. À medida que o script é executado, revise a saída e responda a quaisquer prompts.



Conforme necessário, você pode usar o `tail -f` comando para monitorar o conteúdo do arquivo de log do script (`/var/local/log/sn-remount-volumes.log`). O arquivo de log contém informações mais detalhadas do que a saída da linha de comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
```

your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact support to determine how to recover your data.

```
===== Device /dev/sdd =====
```

```
Mount and unmount device /dev/sdd and checking file system consistency:
```

```
Failed to mount device /dev/sdd
```

```
This device could be an uninitialized disk or has corrupted superblock.
```

```
File system check might take a long time. Do you want to continue? (y or n) [y/N]? y
```

```
Error: File system consistency check retry failed on device /dev/sdd. You can see the diagnosis information in the /var/local/log/sn-remount-volumes.log.
```

This volume could be new or damaged. If you run `sn-recovery-postinstall.sh`, this volume and any data on this volume will be deleted. If you only had two copies of object data, you will temporarily have only a single copy. StorageGRID Webscale will attempt to restore data redundancy by making additional replicated copies or EC fragments, according to the rules in the active ILM policy.

Do not continue to the next step if you believe that the data remaining on this volume cannot be rebuilt from elsewhere in the grid (for example, if your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact support to determine how to recover your data.

```
===== Device /dev/sde =====
```

```
Mount and unmount device /dev/sde and checking file system consistency:
```

```
The device is consistent.
```

```
Check rangedb structure on device /dev/sde:
```

```
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
```

```
This device has all rangedb directories.  
Found LDR node id 12000078, volume number 9 in the volID file  
Error: This volume does not belong to this node. Fix the attached  
volume and re-run this script.
```

Na saída de exemplo, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento tiveram erros.

- `/dev/sdb` Passou a verificação de consistência do sistema de arquivos XFS e teve uma estrutura de volume válida, então foi remontado com sucesso. Os dados em dispositivos que são remontados pelo script são preservados.
- `/dev/sdc` Falha na verificação de consistência do sistema de arquivos XFS porque o volume de armazenamento era novo ou corrompido.
- `/dev/sdd` não foi possível montar porque o disco não foi inicializado ou o superbloco do disco estava corrompido. Quando o script não consegue montar um volume de armazenamento, ele pergunta se você deseja executar a verificação de consistência do sistema de arquivos.
 - Se o volume de armazenamento estiver conectado a um novo disco, responda **N** ao prompt. Você não precisa verificar o sistema de arquivos em um novo disco.
 - Se o volume de armazenamento estiver conectado a um disco existente, responda **Y** ao prompt. Você pode usar os resultados da verificação do sistema de arquivos para determinar a origem da corrupção. Os resultados são guardados no `/var/local/log/sn-remount-volumes.log` arquivo de registro.
- `/dev/sde` Passou a verificação de consistência do sistema de arquivos XFS e tinha uma estrutura de volume válida; no entanto, o ID do nó LDR no arquivo volID não correspondia ao ID para este nó de armazenamento (o `configured LDR noid` exibido na parte superior). Esta mensagem indica que este volume pertence a outro nó de armazenamento.

3. Revise a saída do script e resolva quaisquer problemas.



Se um volume de armazenamento falhou na verificação de consistência do sistema de arquivos XFS ou não pôde ser montado, revise cuidadosamente as mensagens de erro na saída. Você deve entender as implicações da execução `sn-recovery-postinstall.sh` do script nesses volumes.

- a. Verifique se os resultados incluem uma entrada para todos os volumes esperados. Se algum volume não estiver listado, execute novamente o script.
- b. Reveja as mensagens de todos os dispositivos montados. Certifique-se de que não existem erros que indiquem que um volume de armazenamento não pertence a este nó de armazenamento.

No exemplo, a saída para `/dev/sde` inclui a seguinte mensagem de erro:

```
Error: This volume does not belong to this node. Fix the attached  
volume and re-run this script.
```



Se um volume de armazenamento for comunicado como pertencente a outro nó de armazenamento, contacte o suporte técnico. Se você executar `sn-recovery-postinstall.sh` o script, o volume de armazenamento será reformatado, o que pode causar perda de dados.

- c. Se não for possível montar qualquer dispositivo de armazenamento, anote o nome do dispositivo e repare ou substitua o dispositivo.



Deve reparar ou substituir quaisquer dispositivos de armazenamento que não possam ser montados.

Você usará o nome do dispositivo para procurar o ID do volume, que é a entrada necessária quando você executar `repair-data` o script para restaurar os dados do objeto para o volume (o próximo procedimento).

- d. Depois de reparar ou substituir todos os dispositivos não montáveis, execute o `sn-remount-volumes` script novamente para confirmar que todos os volumes de armazenamento que podem ser remontados foram remontados.



Se um volume de armazenamento não puder ser montado ou for formatado incorretamente e você continuar para a próxima etapa, o volume e quaisquer dados no volume serão excluídos. Se você tiver duas cópias de dados de objeto, você terá apenas uma única cópia até concluir o próximo procedimento (restaurando dados de objeto).



Não execute `sn-recovery-postinstall.sh` o script se você acredita que os dados restantes em um volume de armazenamento com falha não podem ser reconstruídos de outro lugar na grade (por exemplo, se sua política de ILM usar uma regra que faça apenas uma cópia ou se os volumes tiverem falhado em vários nós). Em vez disso, entre em Contato com o suporte técnico para determinar como recuperar seus dados.

4. Execute `sn-recovery-postinstall.sh` o script: `sn-recovery-postinstall.sh`

Este script reformata quaisquer volumes de armazenamento que não puderam ser montados ou que foram encontrados para serem formatados incorretamente; reconstrói o banco de dados Cassandra no nó, se necessário; e inicia os serviços no nó Storage Node.

Tenha em atenção o seguinte:

- O script pode levar horas para ser executado.
- Em geral, você deve deixar a sessão SSH sozinha enquanto o script estiver sendo executado.
- Não pressione **Ctrl C** enquanto a sessão SSH estiver ativa.
- O script será executado em segundo plano se ocorrer uma interrupção da rede e terminar a sessão SSH, mas você pode visualizar o progresso da página recuperação.
- Se o nó de armazenamento usar o serviço RSM, o script pode parecer parar por 5 minutos à medida que os serviços do nó são reiniciados. Este atraso de 5 minutos é esperado sempre que o serviço RSM arranque pela primeira vez.



O serviço RSM está presente nos nós de storage que incluem o serviço ADC.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. As reparações ocorrem automaticamente assim que os serviços relacionados ou necessários tiverem sido iniciados. Você pode notar saída de script que menciona "reaper" ou "Cassandra repair." se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. à medida que o `sn-recovery-postinstall.sh` script é executado, monitore a página recuperação no Gerenciador de Grade.

A barra de progresso e a coluna Estágio na página recuperação fornecem um status de alto nível `sn-recovery-postinstall.sh` do script.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
No results found.			

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT	<div style="width: 100%; background-color: #0070C0;"></div>	Recovering Cassandra

Depois que o `sn-recovery-postinstall.sh` script iniciar os serviços no nó, você pode restaurar os dados do objeto para quaisquer volumes de armazenamento que foram formatados pelo script, conforme descrito nesse procedimento.

Informações relacionadas


[Reveja os avisos de recuperação da unidade do sistema Storage Node](#)

[Restaure os dados do objeto para o volume de storage, se necessário](#)

Restaure os dados do objeto para o volume de storage, se necessário

Se o `sn-recovery-postinstall.sh` script for necessário para reformatar um ou mais volumes de storage com falha, você deverá restaurar os dados de objeto para o volume de storage reformatado de outros nós de storage e nós de arquivamento. Essas etapas não são necessárias a menos que um ou mais volumes de armazenamento tenham sido reformatados.

O que você vai precisar

- Você deve ter confirmado que o nó de armazenamento recuperado tem um estado de conexão de **Connected**  na guia **NODES > Overview** no Gerenciador de Grade.

Sobre esta tarefa

Os dados de objetos podem ser restaurados de outros nós de storage, um nó de arquivamento ou um pool de

storage de nuvem, supondo que as regras de ILM da grade tenham sido configuradas de modo que as cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID deverá emitir várias solicitações ao endpoint do pool de armazenamento em nuvem para restaurar os dados do objeto. Antes de executar esse procedimento, entre em Contato com o suporte técnico para obter ajuda na estimativa do período de tempo de recuperação e dos custos associados.
- Se a única cópia restante de um objeto estiver em um nó de arquivo, os dados do objeto serão recuperados do nó de arquivo. A restauração de dados de objetos para um nó de storage a partir de um nó de arquivamento demora mais do que a restauração de cópias de outros nós de storage devido à latência associada a recuperações de sistemas de armazenamento de arquivamento externos.

Sobre o `repair-data` script

Para restaurar os dados do objeto, execute o `repair-data` script. Este script inicia o processo de restauração de dados de objeto e trabalha com a digitalização ILM para garantir que as regras ILM sejam atendidas.

Selecione **dados replicados** ou **dados codificados por apagamento (EC)** abaixo para aprender as diferentes opções para o `repair-data` script, com base se você está restaurando dados replicados ou dados codificados por apagamento. Se você precisar restaurar ambos os tipos de dados, deverá executar ambos os conjuntos de comandos.



Para obter mais informações sobre o `repair-data` script, insira `repair-data --help` a partir da linha de comando do nó Admin principal.

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA) e período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados por apagamento, com base se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Você pode rastrear reparos de dados codificados por apagamento com este comando:

```
repair-data show-ec-repair-status
```



O trabalho de reparação EC reserva temporariamente uma grande quantidade de armazenamento. Os alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparação EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparação EC é concluído, quer o trabalho tenha falhado ou sido bem-sucedido.

Encontre o nome do host para nó de armazenamento

1. Faça login no nó de administração principal:

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

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

2. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte `cat /etc/hosts:`.

Repare os dados se todos os volumes tiverem falhado

Se todos os volumes de armazenamento tiverem falhado, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se apenas alguns volumes tiverem falhado, vá para [Repare os dados se apenas alguns volumes tiverem falhado](#).



Não é possível executar `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em Contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com a `--nodes` opção para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de storage chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. [Monitorar e solucionar problemas](#) Consulte

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `repair-data start-ec-node-repair` comando com a `--nodes` opção para reparar todo o nó de storage.

Este comando repara os dados codificados por apagamento em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Repare os dados se apenas alguns volumes tiverem falhado

Se apenas alguns dos volumes tiverem falhado, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados codificados por apagamento (EC)** ou ambos, com base se você usa dados replicados, dados codificados por apagamento (EC) ou ambos.

Se todos os volumes tiverem falhado, vá para [Repare os dados se todos os volumes tiverem falhado](#).

Introduza as IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estão em uma sequência.

Todos os volumes devem estar no mesmo nó de storage. Se precisar restaurar volumes para mais de um nó de storage, entre em Contato com o suporte técnico.

Dados replicados

Se a grade contiver dados replicados, use o `start-replicated-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em uma sequência: Este comando restaura dados replicados para volumes 0001, 0005 e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



À medida que os dados de objeto são restaurados, o alerta **objetos perdidos** é acionado se o sistema StorageGRID não conseguir localizar dados de objeto replicados. Os alertas podem ser acionados em nós de storage em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Consulte as instruções para monitoramento e solução de problemas do StorageGRID.

Dados codificados para apagamento (EC)

Se sua grade contiver dados codificados por apagamento, use o `start-ec-volume-repair` comando com a `--nodes` opção para identificar o nó. Em seguida, adicione a `--volumes` opção ou `--volume-range`, como mostrado nos exemplos a seguir.

- **Volume único***: Este comando restaura os dados codificados por apagamento para o volume 0007 em um nó de storage chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por apagamento para todos os volumes no intervalo 0004 para 0006 um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em uma sequência: Este comando restaura dados codificados por apagamento para volumes 000A, 000C e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

A `repair-data` operação retorna um único `repair ID` que identifica esta `repair_data` operação. Utilize esta `repair ID` opção para monitorizar o progresso e o resultado `repair_data` da operação. Nenhum outro feedback é retornado à medida que o processo de recuperação é concluído.



As reparações de dados codificados por apagamento podem começar enquanto alguns nós de storage estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Monitorize as reparações

Monitore o status dos trabalhos de reparo, com base se você usa **dados replicados**, **dados codificados por apagamento (EC)** ou ambos.

Dados replicados

- Para determinar se as reparações estão concluídas:
 - a. Selecione **NODES > Storage Node a ser reparado > ILM**.
 - b. Reveja os atributos na seção avaliação. Quando os reparos estiverem concluídos, o atributo **aguardando - All** indica objetos 0D.
- Para monitorizar a reparação em mais detalhes:
 - a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Selecione **Grid > Storage Node a ser reparado > LDR > Data Store**.
 - c. Use uma combinação dos seguintes atributos para determinar, assim como possível, se as reparações replicadas estão concluídas.



As inconsistências do Cassandra podem estar presentes e as reparações falhadas não são rastreadas.

- * Tentativas de reparos (XRPA): **Use este atributo para rastrear o progresso de reparos replicados. Esse atributo aumenta cada vez que um nó de storage tenta reparar um objeto de alto risco. Quando este atributo não aumenta por um período superior ao período de digitalização atual (fornecido pelo atributo *período de digitalização — estimado), significa que a digitalização ILM não encontrou objetos de alto risco que precisam ser reparados em nenhum nó.**



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração ILM.

- **Período de digitalização — estimado (XSCM):** Use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Repairs tented** não aumentar durante um período superior ao período de digitalização atual, é provável que sejam efetuadas reparações replicadas. Note que o período de digitalização pode mudar. O atributo **período de digitalização — estimado (XSCM)** aplica-se a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico de atributos **período de digitalização — estimado** para a grade para determinar um período de tempo apropriado.
- Opcionalmente, para obter uma conclusão percentual estimada para o reparo replicado, adicione a `show-replicated-repair-status` opção ao comando `repair-data`.

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA)** e **período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Para monitorar o reparo de dados codificados por apagamento e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por apagamento:

- Selecione **SUPPORT > Tools > Metrics** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **EC Overview** na seção Grafana. Veja os painéis **Grid EC Job tempo estimado para conclusão** e **Grid EC Job percentage Completed**.

- Use este comando para ver o status de uma operação específica `repair-data`:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilize este comando para listar todas as reparações:

```
repair-data show-ec-repair-status
```

A saída lista informações, `repair ID` incluindo , para todas as reparações anteriores e atualmente em execução.

2. Se a saída mostrar que a operação de reparo falhou, use a `--repair-id` opção para tentar novamente a reparação.

Este comando tenta novamente um reparo de nó com falha, usando a ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado de armazenamento depois de recuperar a unidade de sistema Storage Node

Depois de recuperar a unidade do sistema para um nó de armazenamento, você deve verificar se o estado desejado do nó de armazenamento está definido como on-line e garantir que o estado estará on-line por padrão sempre que o servidor nó de armazenamento for reiniciado.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- O nó de armazenamento foi recuperado e a recuperação de dados está concluída.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Verifique os valores de **nó de armazenamento recuperado > LDR > armazenamento > Estado de armazenamento — desejado** e **Estado de armazenamento — atual**.

O valor de ambos os atributos deve ser Online.

3. Se o estado de armazenamento - desejado estiver definido como somente leitura, execute as seguintes etapas:

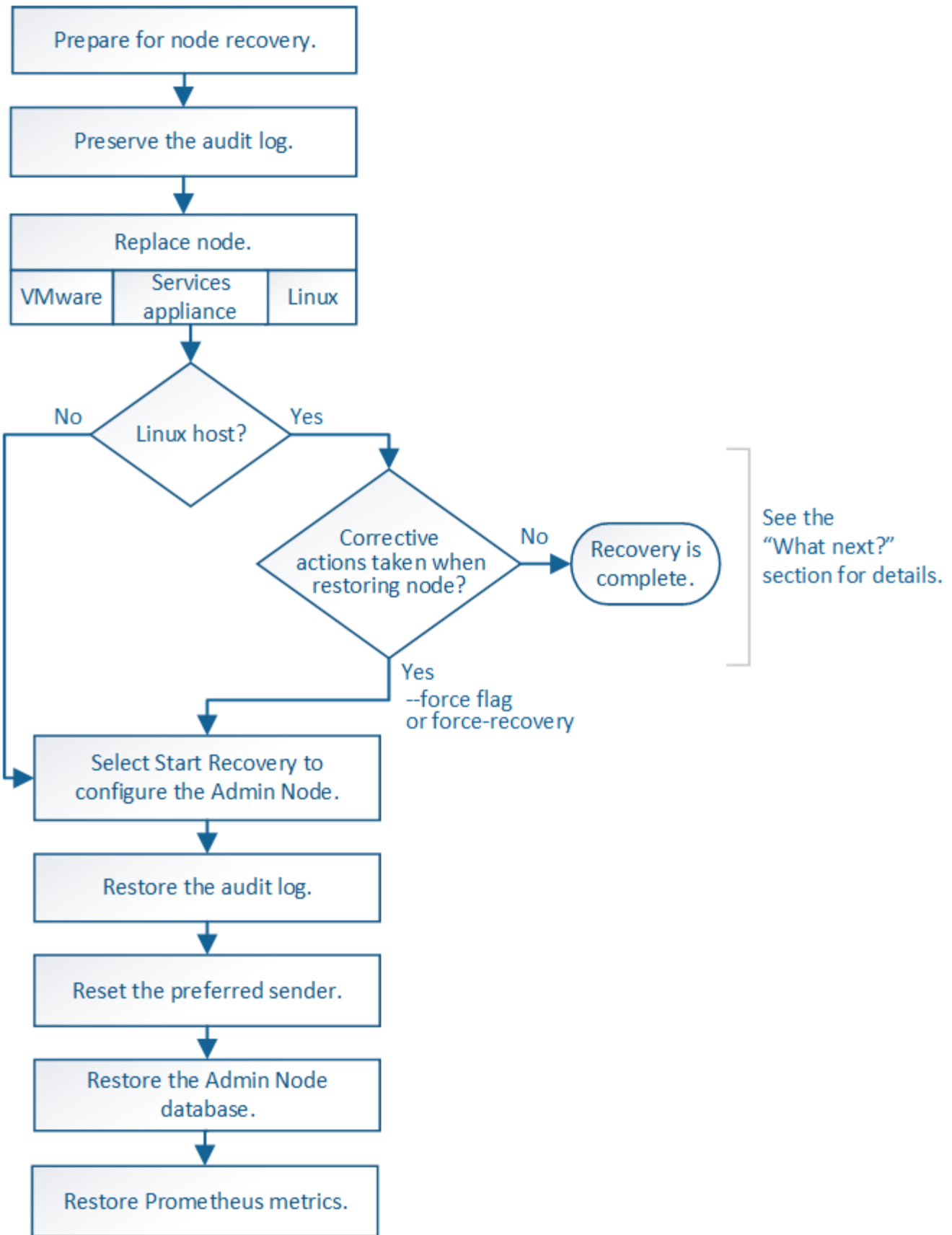
- a. Clique na guia **Configuração**.
- b. Na lista suspensa **Estado de armazenamento - desejado**, selecione **Online**.
- c. Clique em **aplicar alterações**.
- d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — desejado** e **Estado de armazenamento — atual** são atualizados para Online.

Recuperar de falhas no Admin Node

O processo de recuperação para um nó Admin depende se é o nó Admin primário ou um nó Admin não primário.

Sobre esta tarefa

As etapas de alto nível para recuperar um nó de administração primário ou não primário são as mesmas, embora os detalhes das etapas sejam diferentes.



Siga sempre o procedimento de recuperação correto para o nó Admin que está a recuperar. Os procedimentos parecem os mesmos em um nível alto, mas diferem nos detalhes.

Informações relacionadas

Opções

- [Recuperação de falhas do nó de administração principal](#)
- [Recuperação de falhas não primárias no nó de administração](#)

Recuperação de falhas do nó de administração principal

Você deve concluir um conjunto específico de tarefas para recuperar de uma falha de nó de administrador principal. O nó de administração principal hospeda o serviço do nó de gerenciamento de configuração (CMN) para a grade.

Sobre esta tarefa

Um nó de administração principal com falha deve ser substituído imediatamente. O serviço CMN (Configuration Management Node) no nó Admin primário é responsável pela emissão de blocos de identificadores de objetos para a grade. Esses identificadores são atribuídos a objetos à medida que são ingeridos. Novos objetos não podem ser ingeridos a menos que existam identificadores disponíveis. A ingestão de objetos pode continuar enquanto o CMN não estiver disponível porque o fornecimento de identificadores de aproximadamente um mês é armazenado em cache na grade. No entanto, depois que os identificadores armazenados em cache são esgotados, nenhum novo objeto pode ser adicionado.



Você deve reparar ou substituir um nó de administração principal com falha em aproximadamente um mês ou a grade pode perder sua capacidade de ingerir novos objetos. O período de tempo exato depende da sua taxa de ingestão de objetos: Se você precisar de uma avaliação mais precisa do período de tempo para sua grade, entre em Contato com o suporte técnico.

Copiar registros de auditoria do nó de administração principal avariado

Se você for capaz de copiar logs de auditoria do nó de administração principal com falha, você deve preservá-los para manter o Registro da grade de atividade e uso do sistema. Você pode restaurar os logs de auditoria preservados para o nó de administração principal recuperado depois que ele estiver ativo e em execução.

Este procedimento copia os arquivos de log de auditoria do nó de administração com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administrador com falha. Se a implantação tiver apenas um Admin Node, o Admin Node recuperado inicia a gravação de eventos para o log de auditoria em um novo arquivo vazio e os dados gravados anteriormente são perdidos. Se a implantação incluir mais de um nó Admin, você poderá recuperar os logs de auditoria de outro nó Admin.



Se os logs de auditoria não estiverem acessíveis no nó Admin com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Inicie sessão no nó de administração com falha, se possível. Caso contrário, faça login no nó de administração principal ou em outro nó de administração, se disponível.
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

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

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

2. Pare o serviço AMS para impedir que ele crie um novo arquivo de log: `service ams stop`
3. Renomeie o arquivo `audit.log` para que ele não substitua o arquivo existente quando você copiá-lo para o nó Admin recuperado.

Renomeie `audit.log` para um nome de arquivo numerado exclusivo, como `aaaa-mm-dd.txt`.¹ Por exemplo, você pode renomear o arquivo `audit.log` para `2015-10-25.txt`, `cd /var/local/audit/export/`

4. Reinicie o serviço AMS: `service ams start`
5. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

6. Copiar todos os ficheiros de registo de auditoria: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

7. Faça logout como root: `exit`

Substitua o nó de administração principal

Para recuperar um nó de administrador principal, primeiro você deve substituir o hardware físico ou virtual.

Você pode substituir um nó de administrador principal com falha por um nó de administrador principal executado na mesma plataforma ou pode substituir um nó de administrador principal em execução em VMware ou em um host Linux por um nó de administrador principal hospedado em um dispositivo de serviços.

Use o procedimento que corresponde à plataforma de substituição selecionada para o nó. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento irá direcioná-lo para a próxima etapa para a recuperação do nó de administração principal.

Plataforma de substituição	Procedimento
VMware	Substitua um nó VMware
Linux	Substitua um nó Linux
Aparelhos de serviços SG100 e SG1000	Substitua um dispositivo de serviços

Plataforma de substituição	Procedimento
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Configure o nó de administração principal de substituição

O nó de substituição deve ser configurado como nó de administração principal para o seu sistema StorageGRID.

O que você vai precisar

- Para nós de administração primários hospedados em máquinas virtuais, a máquina virtual deve ser implantada, ativada e inicializada.
- Para nós de administração primários hospedados em um dispositivo de serviços, você substituiu o dispositivo e instalou o software. Consulte o guia de instalação do seu aparelho.

[Aparelhos de serviços SG100 e SG1000](#)

- Tem de ter a cópia de segurança mais recente do ficheiro do pacote de recuperação (`sgws-recovery-package-id-revision.zip`).
- Você deve ter a senha de provisionamento.

Passos

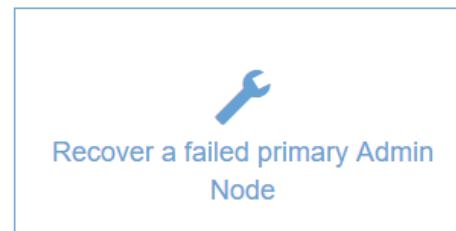
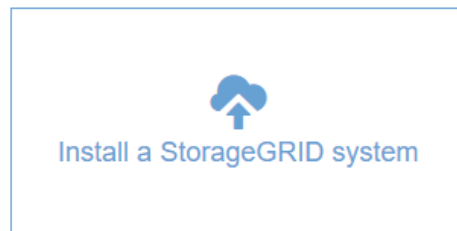
1. Abra o navegador da Web e navegue até https://primary_admin_node_ip.

Install

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



2. Clique em **Recover a failed Primary Admin Node** (recuperar um nó de administrador principal principal)
3. Carregue o backup mais recente do pacote de recuperação:
 - a. Clique em **Procurar**.
 - b. Localize o arquivo mais recente do Pacote de recuperação para o seu sistema StorageGRID e clique em **Open**.
4. Introduza a frase-passe de provisionamento.
5. Clique em **Iniciar recuperação**.

O processo de recuperação começa. O Gerenciador de Grade pode ficar indisponível por alguns minutos à medida que os serviços necessários forem iniciados. Quando a recuperação estiver concluída, a página de início de sessão é apresentada.

6. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID e a confiança da parte confiável para o nó Admin que você recuperou foi configurada para usar o certificado de interface de gerenciamento padrão, atualizar (ou excluir e recriar) a confiança da parte confiável do nó nos Serviços de Federação do ative Directory (AD FS). Use o novo certificado de servidor padrão que foi gerado durante o processo de recuperação do Admin Node.



Para configurar uma confiança de parte confiável, consulte as instruções para administrar o StorageGRID. Para acessar o certificado padrão do servidor, faça login no shell de comando do nó Admin. Vá para `/var/local/mgmt-api` o diretório e selecione o `server.crt` arquivo.

7. Determine se você precisa aplicar um hotfix.
 - a. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
 - b. Selecione **NODES**.

- c. Na lista à esquerda, selecione o nó de administração principal.
- d. Na guia Visão geral, observe a versão exibida no campo **versão do software**.
- e. Selecione qualquer outro nó de grade.
- f. Na guia Visão geral, observe a versão exibida no campo **versão do software**.
 - Se as versões exibidas nos campos **versão do software** forem as mesmas, não será necessário aplicar um hotfix.
 - Se as versões exibidas nos campos **versão do software** forem diferentes, você deve aplicar um hotfix para atualizar o nó de administração primário recuperado para a mesma versão.

Informações relacionadas

[Administrar o StorageGRID](#)

[Procedimento de correção do StorageGRID](#)

Restaure o log de auditoria no nó de administração primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração principal com falha, você pode copiá-lo para o nó de administração principal que está recuperando.

- O Admin Node recuperado deve ser instalado e em execução.
- Você deve ter copiado os logs de auditoria para outro local depois que o nó Admin original falhou.

Se um nó Admin falhar, os logs de auditoria salvos nesse nó Admin são potencialmente perdidos. Pode ser possível preservar dados de perda copiando logs de auditoria do nó de administração com falha e restaurando esses logs de auditoria para o nó de administração recuperado. Dependendo da falha, talvez não seja possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó Admin, você poderá recuperar logs de auditoria de outro nó Admin à medida que os logs de auditoria são replicados para todos os nós Admin.

Se houver apenas um nó Admin e o log de auditoria não puder ser copiado do nó com falha, o nó Admin recuperado inicia a gravação de eventos para o log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó Admin o mais rápido possível para restaurar a funcionalidade de log.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode ignorar estas etapas se qualquer uma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para nós de administrador.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

[Configurar mensagens de auditoria e destinos de log](#) Consulte para obter detalhes.

Passos

1. Faça login no nó de administração recuperado:

- a. Introduza o seguinte comando: `ssh admin@recovery_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.

Depois de iniciar sessão como root, o aviso muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados: `cd /var/local/audit/export`
3. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando solicitado, insira a senha para admin.

4. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.
5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado:
`chown ams-user:bycast *`
6. Faça logout como root: `exit`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

[Administrar o StorageGRID](#)

Redefinir remetente preferido no nó Admin primário recuperado

Se o nó de administração principal que está a recuperar estiver atualmente definido como o remetente preferido de notificações de alerta, notificações de alarme e mensagens AutoSupport, tem de reconfigurar esta definição.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter permissões de acesso específicas.
- O Admin Node recuperado deve ser instalado e em execução.

Passos

1. Selecione **CONFIGURATION > System > Display OPTIONS**.
2. Selecione o Admin Node recuperado na lista suspensa **Preferred Sender**.
3. Clique em **aplicar alterações**.

Informações relacionadas

[Administrar o StorageGRID](#)

Restaurar o banco de dados do nó de administração ao recuperar o nó de administração primário

Se você quiser manter as informações históricas sobre atributos, alarmes e alertas em um nó de administrador principal que falhou, você pode restaurar o banco de dados do nó de administrador. Você só pode restaurar esse banco de dados se o sistema

StorageGRID incluir outro nó de administrador.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as informações históricas armazenadas em seu banco de dados Admin Node serão perdidas. Esta base de dados inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **SUPPORT Tools Grid topology**.

Quando você recupera um Admin Node, o processo de instalação do software cria um banco de dados Admin Node vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados posteriormente.

Se você restaurou um nó de administrador principal e seu sistema StorageGRID tiver outro nó de administrador, você poderá restaurar as informações históricas copiando o banco de dados do nó de administrador de um nó de administrador não primário (o *nó de administrador de origem*) para o nó de administrador principal recuperado. Se o sistema tiver apenas um nó de administração principal, não poderá restaurar a base de dados do nó de administração.



Copiar o banco de dados Admin Node pode levar várias horas. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

1. Faça login no nó de administração de origem:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço MI: `service mi stop`
3. No Admin Node de origem, pare o serviço Management Application Program Interface (mgmt-api):
`service mgmt-api stop`
4. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Parar o serviço MI: `service mi stop`

- c. Pare o serviço mgmt-api: `service mgmt-api stop`
- d. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
- e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
- f. Copie o banco de dados do Admin Node de origem para o Admin Node recuperado:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
- g. Quando solicitado, confirme se você deseja substituir o banco de dados MI no Admin Node recuperado.

O banco de dados e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado.

- h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`

5. Reinicie os serviços no Admin Node de origem: `service servermanager start`

Restaurar as métricas do Prometheus ao recuperar o nó de administração principal

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó de administração principal que falhou. As métricas Prometheus só podem ser restauradas se o seu sistema StorageGRID incluir outro nó Admin.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as métricas mantidas no banco de dados Prometheus no nó Admin serão perdidas. Quando você recupera o Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele Registra as métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó de administrador principal e seu sistema StorageGRID tiver outro nó de administrador, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus de um nó de administrador não primário (o *nó de administrador de origem*) para o nó de administrador principal recuperado. Se o seu sistema tiver apenas um nó Admin principal, não poderá restaurar a base de dados Prometheus.



Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

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

2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Pare o serviço Prometheus: `service prometheus stop`
 - c. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
 - d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - e. Copie o banco de dados Prometheus do nó Admin de origem para o nó Admin recuperado:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
 - f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó Admin recuperado.

O banco de dados Prometheus original e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado. É apresentado o seguinte estado:

Banco de dados clonado, iniciando serviços

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`
4. Reinicie o serviço Prometheus no Admin Node de origem. `service prometheus start`

Recuperação de falhas não primárias no nó de administração

Você deve concluir as tarefas a seguir para se recuperar de uma falha não primária do Admin Node. Um nó de administração hospeda o serviço CMN (Configuration Management Node) e é conhecido como nó de administração principal. Embora você possa ter vários nós de administração, cada sistema StorageGRID inclui apenas um nó de administração principal. Todos os outros nós de administração são nós de administração não primários.

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

Copiar registros de auditoria do nó de administração não primário com falha

Se você conseguir copiar logs de auditoria do nó de administração com falha, você deve preservá-los para manter o Registro da grade de atividade e uso do sistema. Você pode restaurar os logs de auditoria preservados para o nó de administração não primário recuperado depois que ele estiver ativo e em execução.

Este procedimento copia os arquivos de log de auditoria do nó de administração com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administrador com falha. Se a implantação tiver apenas um Admin Node, o Admin Node recuperado inicia a gravação de eventos para o log de auditoria em um novo arquivo vazio e os dados gravados anteriormente são perdidos. Se a implantação incluir mais de um nó Admin, você poderá recuperar os logs de auditoria de outro nó Admin.



Se os logs de auditoria não estiverem acessíveis no nó Admin com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Inicie sessão no nó de administração com falha, se possível. Caso contrário, faça login no nó de administração principal ou em outro nó de administração, se disponível.
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Pare o serviço AMS para impedir que ele crie um novo arquivo de log: `service ams stop`
3. Renomeie o arquivo `audit.log` para que ele não substitua o arquivo existente quando você copiá-lo para o nó Admin recuperado.

Renomeie `audit.log` para um nome de arquivo numerado exclusivo, como `aaaa-mm-dd.txt`.¹ Por exemplo, você pode renomear o arquivo `audit.log` para `2015-10-25.txt`, `1cd /var/local/audit/export/`

4. Reinicie o serviço AMS: `service ams start`
5. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

6. Copiar todos os ficheiros de registo de auditoria: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

7. Faça logout como root: `exit`

Substitua o nó de administração não primário

Para recuperar um nó de administração não primário, primeiro você deve substituir o hardware físico ou virtual.

Você pode substituir um nó de administrador não primário com falha por um nó de administrador não primário executado na mesma plataforma ou substituir um nó de administrador não primário em execução em VMware ou em um host Linux por um nó de administrador não primário hospedado em um dispositivo de serviços.

Use o procedimento que corresponde à plataforma de substituição selecionada para o nó. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento irá direcioná-lo para a próxima etapa para a recuperação do nó de administração não primário.

Plataforma de substituição	Procedimento
VMware	Substitua um nó VMware
Linux	Substitua um nó Linux
Aparelhos de serviços SG100 e SG1000	Substitua um dispositivo de serviços
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecione Iniciar recuperação para configurar o nó de administração não primário

Depois de substituir um nó Admin não primário, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE Tasks Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó para um estado pré-instalado, da seguinte forma:

- **VMware:** Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- *** Linux*:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se você quiser repetir a recuperação após redefinir o procedimento, você deve restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó.

6. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID e a confiança da parte confiável para o nó Admin que você recuperou foi configurada para usar o certificado de interface de gerenciamento padrão, atualizar (ou excluir e recriar) a confiança da parte confiável do nó nos Serviços de Federação do ative Directory (AD FS). Use o novo certificado de servidor padrão que foi gerado durante o processo de recuperação do Admin Node.



Para configurar uma confiança de parte confiável, consulte as instruções para administrar o StorageGRID. Para acessar o certificado padrão do servidor, faça login no shell de comando do nó Admin. Vá para `/var/local/mgmt-api` o diretório e selecione o `server.crt` arquivo.

Informações relacionadas

[Administrar o StorageGRID](#)

[Prepare o aparelho para reinstalação \(apenas substituição da plataforma\)](#)

Restaurar o log de auditoria no nó de administração não primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração não primário com falha, de modo que as informações de log de auditoria histórica sejam mantidas, você pode copiá-lo para o nó de administração não primário que você está recuperando.

- O Admin Node recuperado deve ser instalado e em execução.
- Você deve ter copiado os logs de auditoria para outro local depois que o nó Admin original falhou.

Se um nó Admin falhar, os logs de auditoria salvos nesse nó Admin são potencialmente perdidos. Pode ser possível preservar dados de perda copiando logs de auditoria do nó de administração com falha e restaurando esses logs de auditoria para o nó de administração recuperado. Dependendo da falha, talvez não seja possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó Admin, você poderá recuperar logs de auditoria de outro nó Admin à medida que os logs de auditoria são replicados para todos os nós Admin.

Se houver apenas um nó Admin e o log de auditoria não puder ser copiado do nó com falha, o nó Admin recuperado inicia a gravação de eventos para o log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó Admin o mais rápido possível para restaurar a funcionalidade de log.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode ignorar estas etapas se qualquer uma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para nós de administrador.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

[Configurar mensagens de auditoria e destinos de log](#) Consulte para obter detalhes.

Passos

1. Faça login no nó de administração recuperado:

- a. Digite o seguinte comando `ssh admin@recovery_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.

Depois de iniciar sessão como root, o aviso muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados:

```
cd /var/local/audit/export
```

3. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Quando solicitado, insira a senha para admin.

4. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.
5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado:

```
chown ams-user:bycast *
```

6. Faça logout como root: `exit`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, consulte as instruções para administrar o StorageGRID.

Informações relacionadas

[Administrar o StorageGRID](#)

Reponha o remetente preferido no nó Admin não primário recuperado

Se o nó de administração não primário que está a recuperar estiver atualmente definido como o remetente preferido de notificações de alerta, notificações de alarme e mensagens AutoSupport, tem de reconfigurar esta definição no sistema StorageGRID.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter permissões de acesso específicas.
- O Admin Node recuperado deve ser instalado e em execução.

Passos

1. Selecione **CONFIGURATION > System > Display OPTIONS**.
2. Selecione o Admin Node recuperado na lista suspensa **Preferred Sender**.
3. Clique em **aplicar alterações**.

Informações relacionadas

[Administrar o StorageGRID](#)

Restaure o banco de dados Admin Node ao recuperar o nó Admin não primário

Se você quiser manter as informações históricas sobre atributos, alarmes e alertas em um nó de administração não primário que falhou, você pode restaurar o banco de dados do nó de administração do nó principal.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as informações históricas armazenadas em seu banco de dados Admin Node serão perdidas. Esta base de dados inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **SUPPORT Tools Grid topology**.

Quando você recupera um Admin Node, o processo de instalação do software cria um banco de dados Admin Node vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados posteriormente.

Se você restaurou um nó de administração não primário, você poderá restaurar as informações históricas copiando o banco de dados do nó de administração do nó principal (o *nó de administração de origem*) para o nó recuperado.



Copiar o banco de dados Admin Node pode levar várias horas. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no nó de origem.

1. Faça login no nó de administração de origem:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Execute o seguinte comando a partir do Admin Node de origem. Em seguida, insira a senha de provisionamento, se solicitado. `recover-access-points`
3. No Admin Node de origem, pare o serviço MI: `service mi stop`
4. No Admin Node de origem, pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

iii. Digite o seguinte comando para mudar para root: `su -`

iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

b. Parar o serviço MI: `service mi stop`

c. Pare o serviço mgmt-api: `service mgmt-api stop`

d. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.

f. Copie o banco de dados do Admin Node de origem para o Admin Node recuperado:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Quando solicitado, confirme se você deseja substituir o banco de dados MI no Admin Node recuperado.

O banco de dados e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado.

h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`

6. Reinicie os serviços no Admin Node de origem: `service servermanager start`

Restaurar as métricas do Prometheus ao recuperar o nó de administração não primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó Admin não primário que falhou.

- O Admin Node recuperado deve ser instalado e em execução.
- O sistema StorageGRID deve incluir pelo menos dois nós de administração.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve ter a senha de provisionamento.

Se um nó Admin falhar, as métricas mantidas no banco de dados Prometheus no nó Admin serão perdidas. Quando você recupera o Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele registra as métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó Admin não primário, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus do nó Admin primário (o *source Admin Node*) para o nó Admin recuperado.



Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

1. Faça login no nó de administração de origem:

a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Pare o serviço Prometheus: `service prometheus stop`
 - c. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
 - d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - e. Copie o banco de dados Prometheus do nó Admin de origem para o nó Admin recuperado:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
 - f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó Admin recuperado.

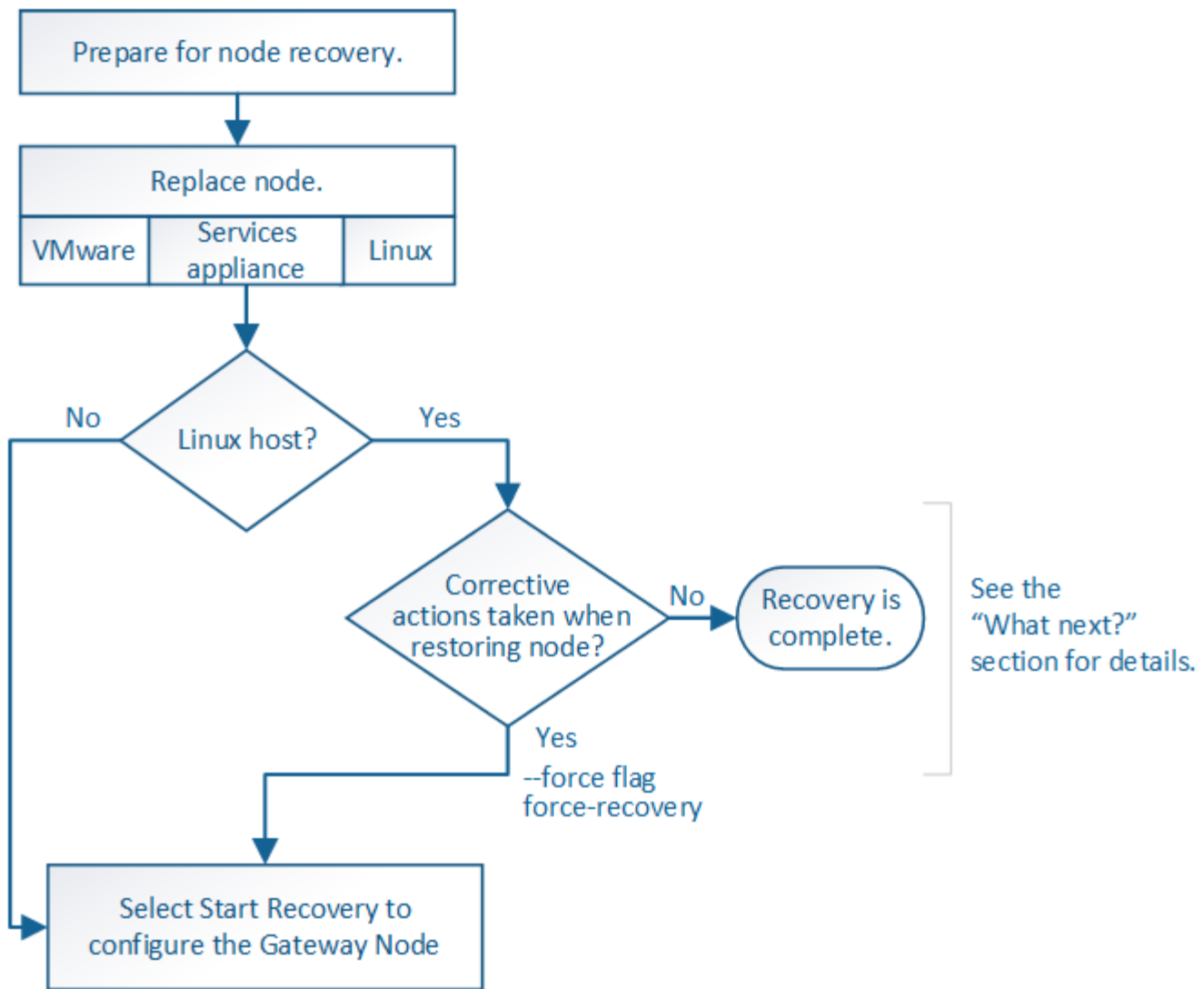
O banco de dados Prometheus original e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado. É apresentado o seguinte estado:

Banco de dados clonado, iniciando serviços

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`
4. Reinicie o serviço Prometheus no Admin Node de origem. `service prometheus start`

Recuperação de falhas do Gateway Node

Você deve concluir uma sequência de tarefas na ordem exata para recuperar de uma falha do Gateway Node.



Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

Substitua o nó de gateway

Você pode substituir um nó de gateway com falha por um nó de gateway executado no mesmo hardware físico ou virtual, ou pode substituir um nó de gateway em execução em VMware ou em um host Linux por um nó de gateway hospedado em um dispositivo de serviços.

O procedimento de substituição do nó que você deve seguir depende de qual plataforma será usada pelo nó de substituição. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento irá direcioná-lo para a próxima etapa para a recuperação do nó de gateway.

Plataforma de substituição	Procedimento
VMware	Substitua um nó VMware
Linux	Substitua um nó Linux

Plataforma de substituição	Procedimento
Aparelhos de serviços SG100 e SG1000	Substitua um dispositivo de serviços
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecione Iniciar recuperação para configurar o Gateway Node

Depois de substituir um nó de gateway, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE Tasks Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó para um estado pré-instalado, da seguinte forma:

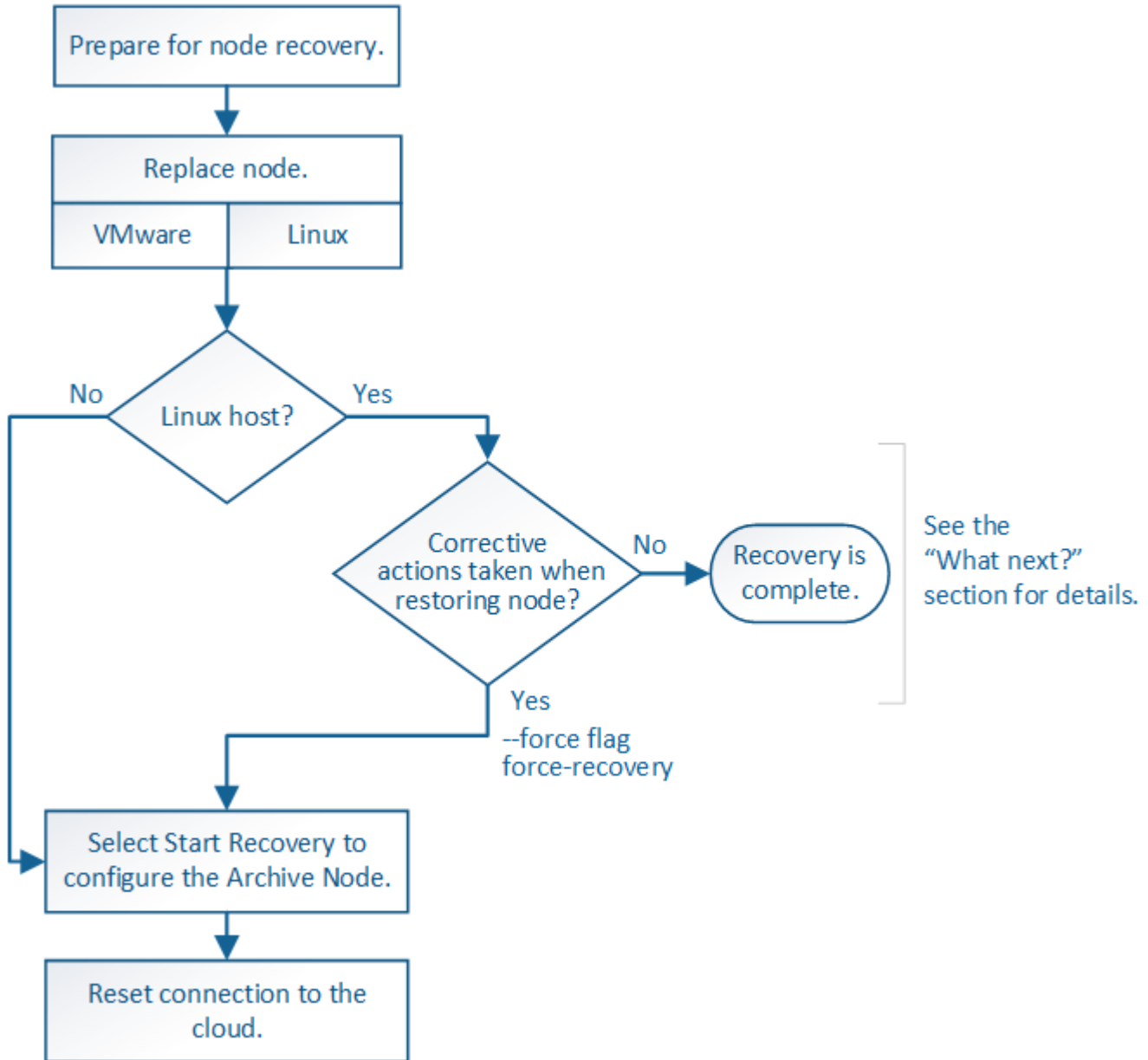
- **VMware:** Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- *** Linux*:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se você quiser repetir a recuperação após redefinir o procedimento, você deve restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó.

Informações relacionadas

Prepare o aparelho para reinstalação (apenas substituição da plataforma)

Recuperação de falhas do nó de arquivo

Você deve concluir uma sequência de tarefas na ordem exata para recuperar de uma falha de nó de arquivo.



Sobre esta tarefa

A recuperação do nó de arquivamento é afetada pelos seguintes problemas:

- Se a política ILM estiver configurada para replicar uma única cópia.

Em um sistema StorageGRID configurado para fazer uma única cópia de objetos, uma falha de nó de arquivo pode resultar em uma perda irreversível de dados. Se houver uma falha, todos esses objetos são perdidos; no entanto, você ainda deve executar procedimentos de recuperação para "limpar" seu sistema StorageGRID e limpar as informações de objetos perdidos do banco de dados.

- Se ocorrer uma falha do nó de arquivamento durante a recuperação do nó de storage.

Se o nó de arquivo falhar ao processar recuperações em massa como parte de uma recuperação do nó de armazenamento, você deve repetir o procedimento para recuperar cópias de dados de objeto para o nó de armazenamento desde o início para garantir que todos os dados de objeto recuperados do nó de arquivo sejam restaurados para o nó de armazenamento.

Substitua o nó de arquivo

Para recuperar um nó de arquivo, você deve primeiro substituir o nó.

Você deve selecionar o procedimento de substituição do nó para sua plataforma. As etapas para substituir um nó são as mesmas para todos os tipos de nós de grade.

Plataforma	Procedimento
VMware	Substitua um nó VMware
Linux	Substitua um nó Linux
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para substituir um nó Linux.

Selecione Iniciar recuperação para configurar o nó de arquivo

Depois de substituir um nó de arquivo, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter implantado e configurado o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE Tasks Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Name	IPv4 Address	State	Recoverable
104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo Info (informações) é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó para um estado pré-instalado, da seguinte forma:

- **VMware:** Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- *** Linux*:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`

Repor a ligação Archive Node à nuvem

Depois de recuperar um nó de arquivo que segmenta a nuvem através da API S3, você precisa modificar as configurações para redefinir as conexões. Um alarme de Estado de replicação de saída (ORSU) é acionado se o nó de arquivo não conseguir recuperar dados de objeto.



Se o seu nó de arquivo se conectar ao armazenamento externo por meio do middleware TSM, o nó será redefinido automaticamente e você não precisará reconfigurar.

O que você vai precisar

Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Target**.
3. Edite o campo **chave de acesso** inserindo um valor incorreto e clique em **aplicar alterações**.
4. Edite o campo **chave de acesso** inserindo o valor correto e clique em **aplicar alterações**.

Todos os tipos de nó de grade: Substitua o nó VMware

Quando você recupera um nó StorageGRID com falha que foi hospedado no VMware, você deve remover o nó com falha e implantar um nó de recuperação.

O que você vai precisar

Você deve ter determinado que a máquina virtual não pode ser restaurada e deve ser substituída.

Sobre esta tarefa

Você usa o VMware vSphere Web Client para remover primeiro a máquina virtual associada ao nó de grade com falha. Em seguida, você pode implantar uma nova máquina virtual.

Este procedimento é apenas uma etapa no processo de recuperação do nó de grade. O procedimento de remoção e implantação de nós é o mesmo para todos os nós da VMware, incluindo nós de administração, nós de storage, nós de gateway e nós de arquivamento.

Passos

1. Faça login no VMware vSphere Web Client.
2. Navegue para a máquina virtual com falha no nó de grade.
3. Anote todas as informações necessárias para implantar o nó de recuperação.
 - a. Clique com o botão direito do Mouse na máquina virtual, selecione a guia **Editar configurações** e observe as configurações em uso.
 - b. Selecione a guia **vApp Options** para exibir e gravar as configurações de rede do nó de grade.
4. Se o nó de grade com falha for um nó de armazenamento, determine se algum dos discos rígidos virtuais usados para armazenamento de dados não está danificado e preserve-os para refixação ao nó de grade recuperado.
5. Desligue a máquina virtual.
6. Selecione **ações > todas as ações do vCenter > Excluir do disco** para excluir a máquina virtual.

7. Implante uma nova máquina virtual para ser o nó de substituição e conecte-a a uma ou mais redes StorageGRID.

Ao implantar o nó, você pode opcionalmente remapear as portas dos nós ou aumentar as configurações de CPU ou memória.



Depois de implantar o novo nó, você pode adicionar novos discos virtuais de acordo com seus requisitos de armazenamento, reanexar quaisquer discos rígidos virtuais preservados do nó de grade com falha removido anteriormente ou ambos.

Para obter instruções:

[Instale o VMware](#) > implantando um nó StorageGRID como uma máquina virtual

8. Conclua o procedimento de recuperação do nó, com base no tipo de nó que está a recuperar.

Tipo de nó	Vá para
Nó de administração principal	Configure o nó de administração principal de substituição
Nó de administração não primário	Selecione Iniciar recuperação para configurar o nó de administração não primário
Nó de gateway	Selecione Iniciar recuperação para configurar o Gateway Node
Nó de storage	Selecione Iniciar recuperação para configurar o nó de armazenamento
Nó de arquivo	Selecione Iniciar recuperação para configurar o nó de arquivo

Todos os tipos de nó de grade: Substitua o nó Linux

Se uma falha exigir que você implante um ou mais novos hosts físicos ou virtuais ou reinstale o Linux em um host existente, você deve implantar e configurar o host de substituição antes de recuperar o nó da grade. Este procedimento é uma etapa do processo de recuperação do nó de grade para todos os tipos de nós de grade.

"Linux" refere-se a uma implantação Red Hat Enterprise Linux, Ubuntu, CentOS ou Debian. Use a ferramenta Matriz de interoperabilidade do NetApp para obter uma lista de versões suportadas.

Este procedimento só é executado como uma etapa no processo de recuperação de nós de storage baseados em software, nós de administração primários ou não primários, nós de gateway ou nós de arquivamento. As etapas são idênticas independentemente do tipo de nó de grade que você está recuperando.

Se mais de um nó de grade estiver hospedado em um host Linux físico ou virtual, você poderá recuperar os nós de grade em qualquer ordem. No entanto, a recuperação de um nó Admin primário primeiro, se presente, impede que a recuperação de outros nós de grade pare, pois eles tentam entrar em Contato com o nó Admin primário para se Registrar para recuperação.

Informações relacionadas

Implante novos hosts Linux

Com algumas exceções, você prepara os novos hosts como fez durante o processo de instalação inicial.

Para implantar hosts Linux novos ou reinstalados físicos ou virtuais, siga o procedimento para preparar os hosts nas instruções de instalação do StorageGRID para o seu sistema operacional Linux.

Este procedimento inclui etapas para realizar as seguintes tarefas:

1. Instale o Linux.
2. Configure a rede host.
3. Configurar o armazenamento do host.
4. Instale o motor do recipiente.
5. Instale o serviço de host do StorageGRID.



Pare depois de concluir a tarefa "Instalar o serviço de host do StorageGRID" nas instruções de instalação. Não inicie a tarefa "implantando nós de grade".

Ao executar estas etapas, observe as seguintes diretrizes importantes:

- Certifique-se de usar os mesmos nomes de interface de host usados no host original.
- Se você usar o storage compartilhado para oferecer suporte aos nós do StorageGRID ou tiver movido algumas ou todas as unidades de disco ou SSDs dos nós com falha para os nós de substituição, será necessário restabelecer os mesmos mapeamentos de storage que estavam presentes no host original. Por exemplo, se você usou WWIDs e aliases `/etc/multipath.conf` como recomendado nas instruções de instalação, certifique-se de usar os mesmos pares alias/WWID no `/etc/multipath.conf` host de substituição.
- Se o nó StorageGRID usar o storage atribuído a partir de um sistema NetApp ONTAP, confirme se o volume não tem uma política de disposição em camadas do FabricPool habilitada. A desativação da disposição em camadas do FabricPool para volumes usados com nós do StorageGRID simplifica a solução de problemas e as operações de storage.



Nunca use o FabricPool para categorizar dados relacionados ao StorageGRID de volta ao próprio StorageGRID. A disposição em camadas de dados do StorageGRID de volta para o StorageGRID aumenta a complexidade operacional e a solução de problemas.

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

Restaure nós de grade para o host

Para restaurar um nó de grade com falha para um novo host Linux, você restaura o arquivo de configuração do nó usando os comandos apropriados.

Ao fazer uma nova instalação, você cria um arquivo de configuração de nó para cada nó de grade a ser instalado em um host. Ao restaurar um nó de grade para um host de substituição, você restaura ou substitui o arquivo de configuração do nó para qualquer nó de grade com falha.

Se algum volume de armazenamento de bloco tiver sido preservado do host anterior, talvez seja necessário executar procedimentos de recuperação adicionais. Os comandos nesta seção ajudam a determinar quais procedimentos adicionais são necessários.

Passos

- [Restaure e valide nós de grade](#)
- [Inicie o serviço de host StorageGRID](#)
- [Recupere nós que não forem iniciados normalmente](#)

Restaure e valide nós de grade

Você deve restaurar os arquivos de configuração de grade para todos os nós de grade com falha e, em seguida, validar os arquivos de configuração de grade e resolver quaisquer erros.

Sobre esta tarefa

Você pode importar qualquer nó de grade que deve estar presente no host, desde que seu `/var/local` volume não tenha sido perdido como resultado da falha do host anterior. Por exemplo, o `/var/local` volume ainda pode existir se você usou armazenamento compartilhado para volumes de dados do sistema StorageGRID, conforme descrito nas instruções de instalação do StorageGRID para o seu sistema operacional Linux. A importação do nó restaura o arquivo de configuração do nó para o host.

Se não for possível importar nós ausentes, você deve recriar seus arquivos de configuração de grade.

Em seguida, você deve validar o arquivo de configuração de grade e resolver quaisquer problemas de rede ou armazenamento que possam ocorrer antes de reiniciar o StorageGRID. Quando você cria novamente o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição usado para o nó que você está recuperando.

Consulte as instruções de instalação para obter mais informações sobre a localização `/var/local` do volume de um nó.

Passos

1. Na linha de comando do host recuperado, liste todos os nós de grade StorageGRID configurados atualmente:
`sudo storagegrid node list`

Se nenhum nó de grade estiver configurado, não haverá saída. Se alguns nós de grade estiverem configurados, espere a saída no seguinte formato:

```
Name                Metadata-Volume
=====
dc1-adm1             /dev/mapper/sgws-adm1-var-local
dc1-gw1              /dev/mapper/sgws-gw1-var-local
dc1-sn1              /dev/mapper/sgws-sn1-var-local
dc1-arcl             /dev/mapper/sgws-arcl-var-local
```

Se alguns ou todos os nós de grade que devem ser configurados no host não estiverem listados, você precisará restaurar os nós de grade ausentes.

2. Para importar nós de grade que têm um `/var/local` volume:

- a. Execute o seguinte comando para cada nó que você deseja importar:

```
sudo storagegrid node import node-var-local-volume-path
```

O `storagegrid node import` comando só é bem-sucedido se o nó de destino foi desligado de forma limpa no host no qual foi executado pela última vez. Se esse não for o caso, você observará um erro semelhante ao seguinte:

```
This node (node-name) appears to be owned by another host (UUID host-uuid).
```

Use the `--force` flag if you are sure import is safe.

- a. Se você vir o erro sobre o nó sendo de propriedade de outro host, execute o comando novamente com o `--force` sinalizador para concluir a importação:

```
sudo storagegrid --force node import node-var-local-volume-path
```



Todos os nós importados com o `--force` sinalizador exigirão etapas de recuperação adicionais antes que eles possam se juntar novamente à grade, como descrito em [O que vem a seguir: Execute etapas adicionais de recuperação, se necessário](#).

3. Para nós de grade que não têm um `/var/local` volume, recrie o arquivo de configuração do nó para restaurá-lo para o host.

Siga as diretrizes em `""criar arquivos de configuração de nó""` nas instruções de instalação.



Quando você cria novamente o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição usado para o nó que você está recuperando. Para implantações Linux, verifique se o nome do arquivo de configuração contém o nome do nó. Você deve usar as mesmas interfaces de rede, bloquear mapeamentos de dispositivos e endereços IP quando possível. Essa prática minimiza a quantidade de dados que precisa ser copiada para o nó durante a recuperação, o que pode tornar a recuperação significativamente mais rápida (em alguns casos, minutos em vez de semanas).



Se você usar quaisquer novos dispositivos de bloco (dispositivos que o nó StorageGRID não usou anteriormente) como valores para qualquer uma das variáveis de configuração que começam `BLOCK_DEVICE_` quando você está recriando o arquivo de configuração para um nó, siga todas as diretrizes no [Corrigir erros de dispositivo de bloco em falta](#).

4. Execute o seguinte comando no host recuperado para listar todos os nós do StorageGRID.

```
sudo storagegrid node list
```

5. Valide o arquivo de configuração de nó para cada nó de grade cujo nome foi mostrado na saída da lista de nós do StorageGRID:

```
sudo storagegrid node validate node-name
```

Você deve resolver quaisquer erros ou avisos antes de iniciar o serviço host do StorageGRID. As seções a

seguir fornecem mais detalhes sobre erros que podem ter significado especial durante a recuperação.

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

[Corrigir erros de interface de rede ausentes](#)

Corrigir erros de interface de rede ausentes

Se a rede host não estiver configurada corretamente ou se um nome estiver incorreto, ocorrerá um erro quando o StorageGRID verificar o mapeamento especificado no `/etc/storagegrid/nodes/node-name.conf` arquivo.

Você pode ver um erro ou aviso correspondente a este padrão:

```
Checking configuration file `/etc/storagegrid/nodes/node-name.conf' para o nó node-name...» ERROR: node-name: GRID_NETWORK_TARGET = host-interface-name Node-name: Interface 'host-interface-name' não existe
```

O erro pode ser reportado para a rede de Grade, a rede Admin ou a rede Cliente. Esse erro significa que o `/etc/storagegrid/nodes/node-name.conf` arquivo mapeia a rede StorageGRID indicada para a interface do host chamada `host-interface-name`, mas não há nenhuma interface com esse nome no host atual.

Se você receber esse erro, verifique se concluiu as etapas em [Implante novos hosts Linux](#). Use os mesmos nomes para todas as interfaces de host que foram usadas no host original.

Se você não conseguir nomear as interfaces do host para corresponder ao arquivo de configuração do nó, você pode editar o arquivo de configuração do nó e alterar o valor do `GRID_network_TARGET`, `ADMIN_network_TARGET` ou `CLIENT_network_TARGET` para corresponder a uma interface de host existente.

Certifique-se de que a interface do host forneça acesso à porta de rede física ou VLAN apropriada e que a interface não faça referência direta a um dispositivo de ligação ou ponte. Você deve configurar uma VLAN (ou outra interface virtual) em cima do dispositivo de ligação no host ou usar um par bridge e Ethernet virtual (vete).

Corrigir erros de dispositivo de bloco em falta

O sistema verifica se cada nó recuperado mapeia para um arquivo especial válido de dispositivo de bloco ou um softlink válido para um arquivo especial de dispositivo de bloco. Se o StorageGRID encontrar mapeamento inválido no `/etc/storagegrid/nodes/node-name.conf` arquivo, um erro de dispositivo de bloco ausente será exibido.

Se observar um erro correspondente a este padrão:

```
Checking configuration file /etc/storagegrid/nodes/node-name.conf for node node-name... ERROR: node-name: BLOCK_DEVICE_PURPOSE = path-name node-name: path-name não existe
```

Isso significa que `/etc/storagegrid/nodes/node-name.conf` mapeia o dispositivo de bloco usado por `node-name` para FINS para o caminho-nome dado no sistema de arquivos Linux, mas não há um arquivo especial válido de dispositivo de bloco ou softlink para um arquivo especial de dispositivo de bloco, nesse local.

Verifique se você concluiu as etapas em [Implante novos hosts Linux](#). Use os mesmos nomes de dispositivos persistentes para todos os dispositivos de bloco que foram usados no host original.

Se você não conseguir restaurar ou recriar o arquivo especial de dispositivo de bloco ausente, você pode alocar um novo dispositivo de bloco com o tamanho e categoria de armazenamento apropriados e editar o arquivo de configuração de nó para alterar o valor de `block_DEVICE_PURPOSE` para apontar para o novo arquivo especial de dispositivo de bloco.

Determine o tamanho e a categoria de armazenamento apropriados nas tabelas na seção "requisitos de armazenamento" das instruções de instalação do seu sistema operacional Linux. Revise as recomendações em ""Configurando o armazenamento do host"" antes de prosseguir com a substituição do dispositivo de bloco.



Se você precisar fornecer um novo dispositivo de armazenamento de bloco para qualquer uma das variáveis de arquivo de configuração começando com `BLOCK_DEVICE_` porque o dispositivo de bloco original foi perdido com o host com falha, verifique se o novo dispositivo de bloco está desformatado antes de tentar outros procedimentos de recuperação. O novo dispositivo de bloco será desformatado se você estiver usando armazenamento compartilhado e tiver criado um novo volume. Se você não tiver certeza, execute o seguinte comando contra qualquer novo dispositivo de armazenamento de bloco arquivos especiais.

CUIDADO:

Execute o seguinte comando apenas para novos dispositivos de armazenamento de bloco. Não execute este comando se você acredita que o armazenamento de bloco ainda contém dados válidos para o nó que está sendo recuperado, pois quaisquer dados no dispositivo serão perdidos.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

Inicie o serviço de host StorageGRID

Para iniciar seus nós do StorageGRID e garantir que eles sejam reiniciados após uma reinicialização do host, você deve habilitar e iniciar o serviço de host do StorageGRID.

1. Execute os seguintes comandos em cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Execute o seguinte comando para garantir que a implantação está em andamento:


```
sudo storagegrid node status node-name
```

Para qualquer nó que retorna um status de não-execução ou parado, execute o seguinte comando:

```
sudo storagegrid node start node-name
```

3. Se você já ativou e iniciou o serviço de host StorageGRID (ou se não tiver certeza se o serviço foi ativado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Recupere nós que não forem iniciados normalmente

Se um nó StorageGRID não se juntar novamente à grade normalmente e não aparecer como recuperável, ele pode estar corrompido. Você pode forçar o nó para o modo de recuperação.

Para forçar o nó para o modo de recuperação:

```
sudo storagegrid node force-recovery node-name
```



Antes de emitir este comando, confirme se a configuração de rede do nó está correta; pode ter falhado em reingressar na grade devido a mapeamentos de interface de rede incorretos ou um endereço IP ou gateway de rede de Grade incorreto.



Depois de emitir o `storagegrid node force-recovery node-name` comando, você deve executar etapas adicionais de recuperação para *node-name*.

Informações relacionadas

[O que vem a seguir: Execute etapas adicionais de recuperação, se necessário](#)

O que vem a seguir: Execute etapas adicionais de recuperação, se necessário

Dependendo das ações específicas que você executou para executar os nós do StorageGRID no host de substituição, talvez seja necessário executar etapas adicionais de recuperação para cada nó.

A recuperação do nó está concluída se você não precisar tomar nenhuma ação corretiva enquanto você substituiu o host Linux ou restaurou o nó de grade com falha para o novo host.

Ações corretivas e próximas etapas

Durante a substituição do nó, talvez seja necessário executar uma destas ações corretivas:

- Você teve que usar o `--force` sinalizador para importar o nó.
- Para qualquer `<PURPOSE>`, o valor `BLOCK_DEVICE_<PURPOSE>` da variável de arquivo de configuração refere-se a um dispositivo de bloco que não contém os mesmos dados que fez antes da falha do host.
- Você emitiu `storagegrid node force-recovery node-name` para o nó.

- Você adicionou um novo dispositivo de bloco.

Se você tomou **alguma** dessas ações corretivas, você deve executar etapas adicionais de recuperação.

Tipo de recuperação	Próximo passo
Nó de administração principal	Configure o nó de administração principal de substituição
Nó de administração não primário	Selecione Iniciar recuperação para configurar o nó de administração não primário
Nó de gateway	Selecione Iniciar recuperação para configurar o Gateway Node
Nó de arquivo	Selecione Iniciar recuperação para configurar o nó de arquivo
Nó de storage (baseado em software): <ul style="list-style-type: none"> • Se você tivesse que usar o <code>--force</code> sinalizador para importar o nó, ou você emitiu <code>storagegrid node force-recovery node-name</code> • Se você teve que fazer uma reinstalação completa do nó ou você precisava restaurar <code>/var/local</code> 	Selecione Iniciar recuperação para configurar o nó de armazenamento
Nó de storage (baseado em software): <ul style="list-style-type: none"> • Se você adicionou um novo dispositivo de bloco. • Se, para qualquer <code><PURPOSE></code>, o valor <code>BLOCK_DEVICE_<PURPOSE></code> da variável de arquivo de configuração se referir a um dispositivo de bloco que não contém os mesmos dados que fez antes da falha do host. 	Recuperar de uma falha no volume de armazenamento em que a unidade do sistema está intacta

Substitua o nó com falha pelo dispositivo de serviços

Você pode usar um dispositivo de serviços SG100 ou SG1000 para recuperar um nó de gateway com falha, um nó de administrador não primário com falha ou um nó de administrador principal com falha hospedado em VMware, um host Linux ou um dispositivo de serviços. Este procedimento é uma etapa do procedimento de recuperação do nó de grade.

O que você vai precisar

- Você deve ter determinado que uma das seguintes situações é verdadeira:
 - A máquina virtual que hospeda o nó não pode ser restaurada.
 - O host físico ou virtual do Linux para o nó de grade falhou e deve ser substituído.

- O dispositivo de serviços que hospeda o nó de grade deve ser substituído.
- Você deve certificar-se de que a versão do Instalador de dispositivos StorageGRID no utilitário de serviços corresponde à versão de software do seu sistema StorageGRID, conforme descrito em instalação e manutenção de hardware para verificar e atualizar a versão do Instalador de dispositivos StorageGRID.

[Aparelhos de serviços SG100 e SG1000](#)



Não implante um dispositivo de serviço SG100 e SG1000 no mesmo local. Pode resultar em performance imprevisível.

Sobre esta tarefa

Você pode usar um dispositivo de serviços SG100 ou SG1000 para recuperar um nó de grade com falha nos seguintes casos:

- O nó com falha foi hospedado no VMware ou Linux (mudança de plataforma)
- O nó com falha foi hospedado em um dispositivo de serviços (substituição da plataforma)

Instalar dispositivo de serviços (somente mudança de plataforma)

Quando você estiver recuperando um nó de grade com falha hospedado no VMware ou em um host Linux e estiver usando um dispositivo de serviços SG100 ou SG1000 para o nó de substituição, primeiro instale o novo hardware do dispositivo usando o mesmo nome do nó que o nó com falha.

Você deve ter as seguintes informações sobre o nó com falha:

- **Nome do nó:** Você deve instalar o utilitário de serviços usando o mesmo nome do nó que o nó com falha.
- **Endereços IP:** Você pode atribuir ao utilitário de serviços os mesmos endereços IP que o nó com falha, que é a opção preferida, ou você pode selecionar um novo endereço IP não utilizado em cada rede.

Execute este procedimento somente se você estiver recuperando um nó com falha hospedado no VMware ou Linux e estiver substituindo-o por um nó hospedado em um dispositivo de serviços.

1. Siga as instruções para instalar um novo dispositivo de serviços SG100 ou SG1000.
2. Quando for solicitado um nome de nó, use o nome do nó do nó com falha.

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

Preparar o aparelho para reinstalação para reinstalação (apenas substituição da plataforma)

Ao recuperar um nó de grade hospedado em um dispositivo de serviços, primeiro você precisa preparar o dispositivo para reinstalação do software StorageGRID.

Execute este procedimento somente se você estiver substituindo um nó com falha hospedado em um dispositivo de serviços. Não siga estas etapas se o nó com falha tiver sido originalmente hospedado no VMware ou em um host Linux.

1. Inicie sessão no nó da grelha com falha:

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

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

2. Prepare o aparelho para a instalação do software StorageGRID. Introduza: `sgareinstall`
3. Quando solicitado a continuar, digite: `y`

O aparelho reinicializa e sua sessão SSH termina. Normalmente, demora cerca de 5 minutos para que o Instalador de dispositivos StorageGRID fique disponível, embora em alguns casos você possa precisar esperar até 30 minutos.

O utilitário de serviços é redefinido e os dados no nó da grade não estão mais acessíveis. Os endereços IP configurados durante o processo de instalação original devem permanecer intactos; no entanto, é recomendável que você confirme isso quando o procedimento for concluído.

Depois de executar o `sgareinstall` comando, todas as contas, senhas e chaves SSH provisionadas pelo StorageGRID são removidas e novas chaves de host são geradas.

Inicie a instalação do software no dispositivo de serviços

Para instalar um nó de gateway ou nó de administrador em um dispositivo de serviços SG100 ou SG1000, use o Instalador de dispositivos StorageGRID, que está incluído no dispositivo.

O que você vai precisar

- O dispositivo deve ser instalado em um rack, conetado às redes e ligado.
- Os links de rede e endereços IP devem ser configurados para o dispositivo usando o Instalador de dispositivos StorageGRID.
- Se você estiver instalando um nó de gateway ou um nó de administrador não primário, você saberá o endereço IP do nó de administrador principal para a grade StorageGRID.
- Todas as sub-redes de rede de grade listadas na página Configuração IP do Instalador de dispositivos StorageGRID devem ser definidas na Lista de sub-redes de rede de grade no nó de administração principal.

Para obter instruções para concluir estas tarefas de pré-requisito, consulte as instruções de instalação e manutenção de um dispositivo de serviços SG100 ou SG1000.

- Você deve estar usando um [navegador da web suportado](#).
- Você deve saber um dos endereços IP atribuídos ao dispositivo. Você pode usar o endereço IP da rede Admin, da rede Grid ou da rede Client.
- Se você está instalando um nó de administrador principal, você tem os arquivos de instalação Ubuntu ou Debian para esta versão do StorageGRID disponíveis.



Uma versão recente do software StorageGRID é pré-carregada no equipamento de serviços durante o fabrico. Se a versão pré-carregada do software corresponder à versão que está a ser utilizada na implementação do StorageGRID, não necessita dos ficheiros de instalação.

Sobre esta tarefa

Para instalar o software StorageGRID em um dispositivo de serviços SG100 ou SG1000:

- Para um nó de administração principal, especifique o nome do nó e, em seguida, carregue os pacotes de software apropriados (se necessário).
- Para um nó de administração não primário ou um nó de gateway, especifique ou confirme o endereço IP do nó de administração principal e o nome do nó.
- Inicie a instalação e aguarde à medida que os volumes estão configurados e o software está instalado.
- No decorrer do processo, a instalação é interrompida. Para retomar a instalação, você deve entrar no Gerenciador de Grade e configurar o nó pendente como um substituto para o nó com falha.
- Depois de configurar o nó, o processo de instalação do appliance é concluído e o appliance é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do dispositivo de serviços SG100 ou SG1000.

`https://Controller_IP:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

This Node

Node type: Gateway ▾

Node name: NetApp-SGA

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery Uncheck to manually enter the Primary Admin Node IP

Connection state: Admin Node discovery is in progress

Cancel Save

Installation

Current state: Unable to start installation. The Admin Node connection is not ready.

Start installation

2. Para instalar um nó de administração principal:

- a. Na seção este nó, para **tipo de nó**, selecione **Admin principal**.
- b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.
- c. Na seção Instalação, verifique a versão do software listada no estado atual

Se a versão do software que está pronta para instalar estiver correta, avance para o [Etapa de instalação](#).

- d. Se você precisar fazer o upload de uma versão diferente do software, no menu **Avançado**, selecione **carregar software StorageGRID**.

A página carregar software StorageGRID é exibida.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version None

Package Name None

Upload StorageGRID Installation Software

Software
Package

Browse

Checksum File

Browse

- a. Clique em **Procurar** para carregar o **Pacote de software** e o **Arquivo de soma de verificação** para o software StorageGRID.

Os arquivos são carregados automaticamente depois de selecioná-los.

- b. Clique em **Início** para retornar à página inicial do instalador do StorageGRID Appliance.

3. Para instalar um nó de gateway ou um nó de administração não primário:

- a. Na seção este nó, para **tipo de nó**, selecione **Gateway** ou **Admin não primário**, dependendo do tipo de nó que você está restaurando.
- b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.
- c. Na seção conexão nó de administrador principal, determine se você precisa especificar o endereço IP do nó de administrador principal.

O Instalador do StorageGRID Appliance pode descobrir esse endereço IP automaticamente, assumindo que o nó de administrador principal, ou pelo menos um outro nó de grade com ADMIN_IP configurado, está presente na mesma sub-rede.

- d. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Descrição
Entrada de IP manual	<ol style="list-style-type: none"> a. Desmarque a caixa de seleção Ativar descoberta de nó de administrador. b. Introduza o endereço IP manualmente. c. Clique em Salvar. d. Aguarde enquanto o estado de conexão para o novo endereço IP se torna "pronto".

Opção	Descrição
Detecção automática de todos os nós de administração principal conectados	<ol style="list-style-type: none"> Marque a caixa de seleção Enable Admin Node Discovery (Ativar descoberta de nó de administrador). Na lista de endereços IP descobertos, selecione o nó de administração principal para a grade em que esse dispositivo de serviços será implantado. Clique em Salvar. Aguarde enquanto o estado de conexão para o novo endereço IP se torna "pronto".

- na seção Instalação, confirme se o estado atual está Pronto para iniciar a instalação do nome do nó e se o botão **Start Installation** está ativado.

Se o botão **Start Installation** (Iniciar instalação) não estiver ativado, poderá ser necessário alterar a configuração da rede ou as definições da porta. Para obter instruções, consulte as instruções de instalação e manutenção do seu aparelho.

- Na página inicial do Instalador de dispositivos StorageGRID, clique em **Iniciar instalação**.

O estado atual muda para ""Instalação está em andamento"" e a página Instalação do Monitor é exibida.



Se você precisar acessar a página Instalação do Monitor manualmente, clique em **Instalação do Monitor** na barra de menus.

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)




Monitorar a instalação do dispositivo de serviços

O Instalador de dispositivos StorageGRID fornece o status até que a instalação esteja concluída. Quando a instalação do software estiver concluída, o dispositivo é reinicializado.

- Para monitorar o progresso da instalação, clique em **Monitor Installation** na barra de menus.

A página Instalação do monitor mostra o progresso da instalação.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

A barra de status azul indica qual tarefa está atualmente em andamento. As barras de estado verdes indicam tarefas concluídas com êxito.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver reexecutando uma instalação, todas as tarefas que não precisam ser executadas novamente serão mostradas com uma barra de status verde e um status de "pulado".

2. Reveja o progresso das duas primeiras fases de instalação.

◦ 1. Configurar armazenamento

Durante este estágio, o instalador limpa qualquer configuração existente das unidades e configura as configurações do host.

◦ 2. Instale o os

Durante esta fase, o instalador copia a imagem base do sistema operativo para o StorageGRID do nó de administração principal para o dispositivo ou instala o sistema operativo base a partir do pacote de instalação do nó de administração principal.

3. Continue a monitorizar o progresso da instalação até que ocorra uma das seguintes situações:

- Para nós de Gateway de dispositivo ou nós de administração de dispositivo não-primário, o estágio **Install StorageGRID** é pausado e uma mensagem é exibida no console incorporado, solicitando que você aprove esse nó no nó de administrador usando o Gerenciador de grade.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```


- Para os nós de administração principais do dispositivo, uma quinta fase (Load StorageGRID Installer) é exibida. Se a quinta fase estiver em andamento por mais de 10 minutos, atualize a página manualmente.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Vá para a próxima etapa do processo de recuperação para o tipo de nó de grade de dispositivo que você está recuperando.

Tipo de recuperação	Referência
Nó de gateway	Selecione Iniciar recuperação para configurar o Gateway Node
Nó de administração não primário	Selecione Iniciar recuperação para configurar o nó de administração não primário
Nó de administração principal	Configure o nó de administração principal de substituição

Como a recuperação do local é realizada pelo suporte técnico

Se um local StorageGRID inteiro falhar ou se vários nós de storage falharem, entre em Contato com o suporte técnico. O suporte técnico avaliará sua situação, desenvolverá um plano de recuperação e recuperará os nós ou o local com falha de uma maneira que atenda aos objetivos de negócios, otimize o tempo de recuperação e evite a perda desnecessária de dados.



A recuperação do local só pode ser realizada por suporte técnico.

Os sistemas StorageGRID são resilientes a uma grande variedade de falhas e você pode executar com sucesso muitos procedimentos de recuperação e manutenção. No entanto, é difícil criar um procedimento simples e generalizado de recuperação do local, porque as etapas detalhadas dependem de fatores específicos para sua situação. Por exemplo:

- **Seus objetivos de negócios:** Após a perda completa de um site da StorageGRID, você deve avaliar a melhor forma de atender aos seus objetivos de negócios. Por exemplo, você deseja reconstruir o site perdido no local? Pretende substituir o site Lost StorageGRID numa nova localização? A situação de cada cliente é diferente, e seu plano de recuperação deve ser projetado para atender às suas prioridades.
- **Natureza exata da falha:** Antes de iniciar uma recuperação do local, é importante estabelecer se algum nó no local com falha está intacto ou se algum nó de armazenamento contém objetos recuperáveis. Se você reconstruir nós ou volumes de storage que contenham dados válidos, poderá ocorrer perda

desnecessária de dados.

- **Ative ILM policy:** O número, tipo e localização das cópias de objetos em sua grade é controlado por sua política ILM ativa. As especificidades da sua política de ILM podem afetar a quantidade de dados recuperáveis, bem como as técnicas específicas necessárias para a recuperação.



Se um site contém a única cópia de um objeto e o site é perdido, o objeto é perdido.

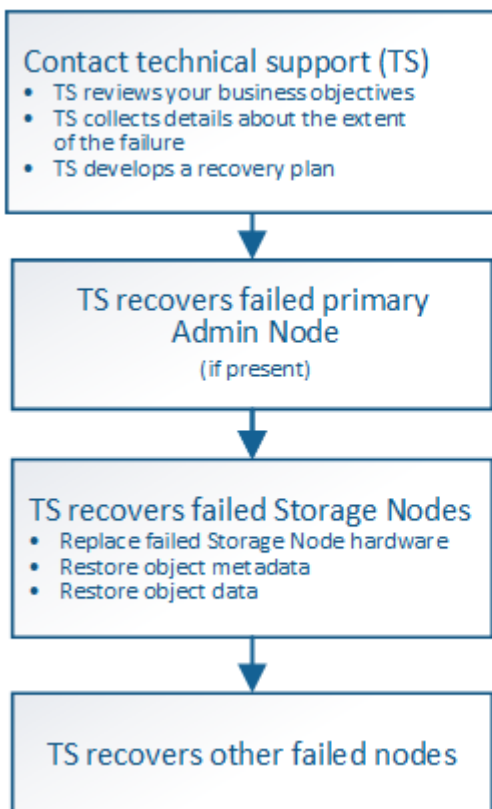
- **Consistência de bucket (ou container):** O nível de consistência aplicado a um bucket (ou container) afeta se o StorageGRID replica totalmente os metadados de objetos para todos os nós e sites antes de informar ao cliente que a ingestão de objetos foi bem-sucedida. Se o seu nível de consistência permitir consistência, alguns metadados de objetos podem ter sido perdidos na falha do site. Isso pode afetar a quantidade de dados recuperáveis e, potencialmente, os detalhes do procedimento de recuperação.
- **Histórico de alterações recentes:** Os detalhes do seu procedimento de recuperação podem ser afetados se algum procedimento de manutenção estava em andamento no momento da falha ou se alguma alteração recente foi feita à sua política de ILM. O suporte técnico deve avaliar o histórico recente de sua grade, bem como sua situação atual antes de iniciar uma recuperação do local.

Visão geral da recuperação do local

Esta é uma visão geral do processo que o suporte técnico usa para recuperar um site com falha.



A recuperação do local só pode ser realizada por suporte técnico.



Caution: Do not use the recovery procedures designed for a single failed Storage Node. Data loss will occur.

1. Entre em Contato com o suporte técnico.

O suporte técnico faz uma avaliação detalhada da falha e trabalha com você para analisar seus objetivos de negócios. Com base nessas informações, o suporte técnico desenvolve um plano de recuperação adaptado à sua situação.

2. O suporte técnico recupera o nó de administração principal se ele tiver falhado.
3. O suporte técnico recupera todos os nós de storage, seguindo este resumo:
 - a. Substitua o hardware do nó de armazenamento ou as máquinas virtuais conforme necessário.
 - b. Restaurar metadados de objetos para o site com falha.
 - c. Restaure os dados do objeto para os nós de storage recuperados.



A perda de dados ocorrerá se os procedimentos de recuperação para um único nó de armazenamento com falha forem usados.



Quando um site inteiro falhou, comandos especializados são necessários para restaurar objetos e metadados de objetos com sucesso.

4. O suporte técnico recupera outros nós com falha.

Depois que os metadados e os dados do objeto tiverem sido recuperados, os nós de Gateway com falha, os nós de administrador não primários ou os nós de arquivo podem ser recuperados usando procedimentos padrão.

Informações relacionadas

[Desativação do site](#)

Procedimento de desativação

Você pode executar um procedimento de desativação para remover permanentemente nós de grade ou um site inteiro do sistema StorageGRID.

Para remover um nó de grade ou um local, execute um dos seguintes procedimentos de desativação:

- Execute um **node deactivation** para remover um ou mais nós, que podem estar em um ou mais sites. Os nós removidos podem estar online e conectados ao sistema StorageGRID, ou podem estar offline e desconectados.
- Execute um **desativação do site conectado** para remover um site no qual todos os nós estão conectados ao StorageGRID.
- Execute um **Desligamento do local desconectado** para remover um local no qual todos os nós são desconectados do StorageGRID.



Antes de executar uma desativação do site desconectada, você deve entrar em Contato com seu representante da conta do NetApp. O NetApp revisará seus requisitos antes de ativar todas as etapas no assistente do site de desintegração. Você não deve tentar uma desativação de site desconectada se você acredita que pode ser possível recuperar o site ou recuperar dados de objeto do site.

Se um site contiver uma mistura de nós conectados (✓) e desconectados (☾ ou ⚙), você deverá colocar todos os nós offline novamente online.



Se precisar executar um segundo procedimento de manutenção, você pode [Interrompa o procedimento de desativação enquanto os nós de storage estão sendo removidos](#). O botão **Pausa** é ativado somente quando os estágios de avaliação ILM ou desativação de dados codificados por apagamento forem alcançados; no entanto, a avaliação ILM (migração de dados) continuará a ser executada em segundo plano. Depois de concluído o segundo procedimento de manutenção, pode retomar a desativação.

Informações relacionadas

[Desativação do nó de grade](#)

[Desativação do site](#)

Desativação do nó de grade

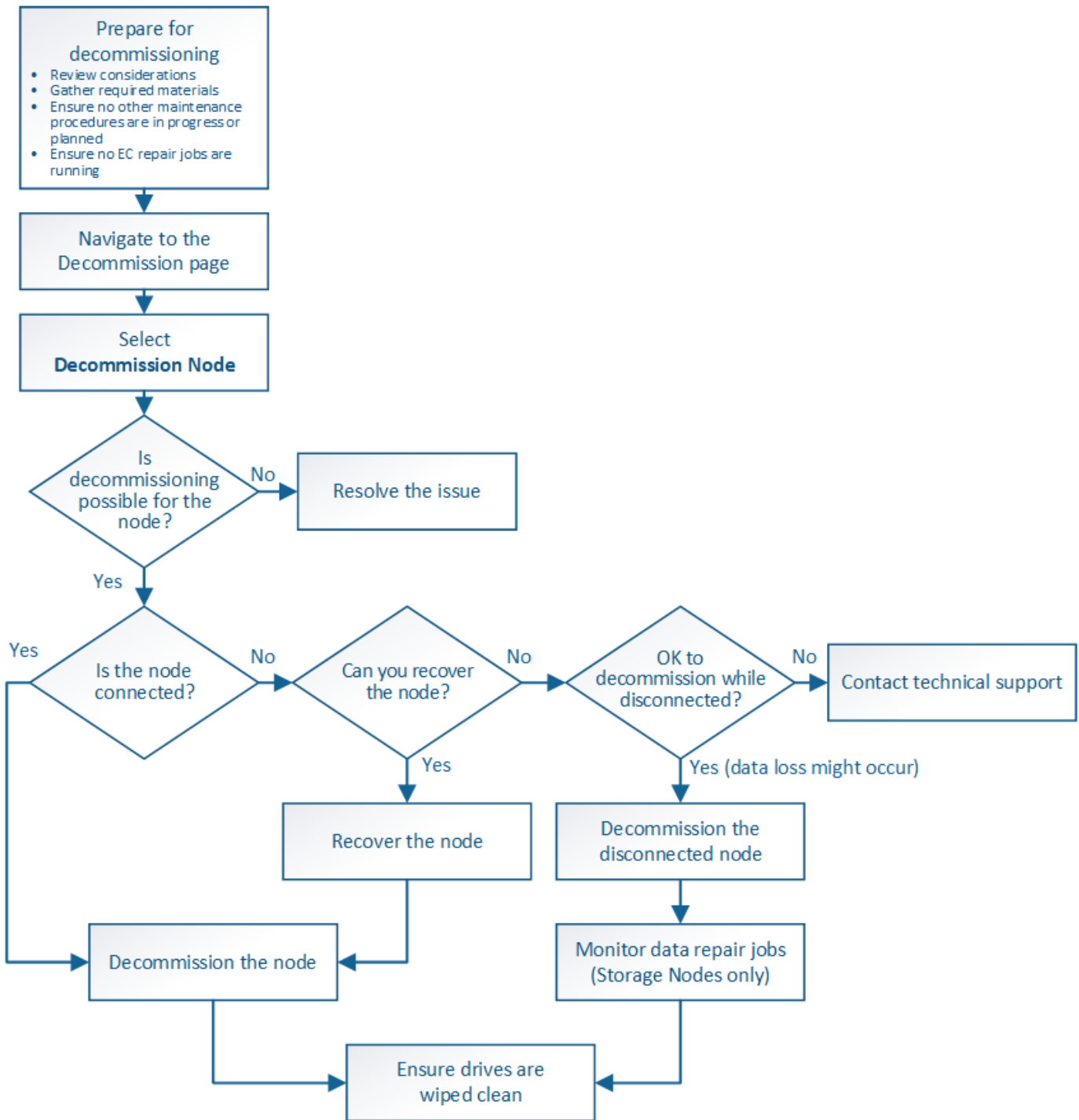
Você pode usar o procedimento de desativação do nó para remover um ou mais nós de storage, nós de gateway ou nós de administração não primários em um ou mais locais. Não é possível desativar o nó de administração principal ou um nó de arquivo.

Em geral, você deve desativar os nós de grade somente enquanto eles estiverem conectados ao sistema StorageGRID e todos os nós estiverem em estado normal (tenha ícones verdes nas páginas **NÓS** e na página **NÓS de desintegração**). No entanto, se necessário, você pode desativar um nó de grade que está desconectado. Antes de remover um nó desconectado, certifique-se de entender as implicações e restrições desse processo.

Use o procedimento de desativação do nó quando qualquer uma das seguintes situações for verdadeira:

- Você adicionou um nó de storage maior ao sistema e deseja remover um ou mais nós de storage menores, preservando ao mesmo tempo objetos.
- Você exige menos storage total.
- Você não precisa mais de um nó de gateway.
- Você não precisa mais de um nó de administrador não primário.
- Sua grade inclui um nó desconectado que você não pode recuperar ou trazer de volta on-line.

O fluxograma mostra as etapas de alto nível para a desativação de nós de grade.



Prepare-se para desativar os nós de grade

Você deve analisar as considerações para remover nós de grade e confirmar que nenhum trabalho de reparo está ativo para dados codificados de apagamento.

Considerações para desativação do nó de grade

Antes de iniciar este procedimento para desativar um ou mais nós, você deve entender as implicações da remoção de cada tipo de nó. Após a desativação bem-sucedida de um nó, seus serviços serão desativados e o nó será desligado automaticamente.

Você não pode desativar um nó se isso deixar o StorageGRID em um estado inválido. As seguintes regras são aplicadas:

- Não é possível desativar o nó de administração principal.
- Não é possível desativar os nós de arquivo.
- Não é possível desativar um nó de administrador ou um nó de gateway se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA).
- Não é possível desativar um nó de armazenamento se a sua remoção afetar o quórum de ADC.
- Não é possível desativar um nó de storage se for necessário para a política ILM ativa.
- Você não deve desativar mais de 10 nós de storage em um único procedimento de nó de compactação.
- Não é possível desativar um nó conectado se a grade incluir nenhum nó desconectado (nós cuja integridade é desconhecida ou administrativamente inoperante). Primeiro, você deve desativar ou recuperar os nós desconectados.
- Se sua grade contiver vários nós desconectados, o software exige que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.
- Se um nó desconectado não puder ser removido (por exemplo, um nó de armazenamento necessário para o quórum de ADC), nenhum outro nó desconectado poderá ser removido.
- Se você quiser substituir um dispositivo mais antigo por um dispositivo mais novo, considere [clonar o nó do dispositivo](#) em vez de desativar o nó antigo e adicionar o novo nó em uma expansão.



Não remova a máquina virtual de um nó de grade ou outros recursos até que seja instruído a fazê-lo em procedimentos de desativação.

Considerações para desativação do nó de administrador ou do nó de gateway

Reveja as seguintes considerações antes de desativar um nó de administrador ou um nó de gateway.

- O procedimento de desativação requer acesso exclusivo a alguns recursos do sistema, portanto, você deve confirmar que nenhum outro procedimento de manutenção está sendo executado.
- Não é possível desativar o nó de administração principal.
- Não é possível desativar um nó de administrador ou um nó de gateway se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA). Primeiro, é necessário remover as interfaces de rede do grupo HA. Consulte as instruções para administrar o StorageGRID.
- Conforme necessário, você pode alterar com segurança a política de ILM ao desativar um nó de gateway ou um nó de administrador.
- Se você desativar um nó de administrador e o logon único (SSO) estiver ativado para seu sistema StorageGRID, lembre-se de remover a confiança de parte confiável do nó dos Serviços de Federação do ative Directory (AD FS).

Informações relacionadas

[Administrar o StorageGRID](#)

Considerações para desativação do nó de storage

Se você pretende desativar um nó de storage, deve entender como o StorageGRID gerencia os dados e os metadados do objeto nesse nó.

As considerações e restrições a seguir se aplicam ao descomissionamento de nós de storage:

- O sistema deve, em todos os momentos, incluir nós de armazenamento suficientes para satisfazer os requisitos operacionais, incluindo o quórum de ADC e a política de ILM ativa. Para satisfazer essa restrição, talvez seja necessário adicionar um novo nó de armazenamento em uma operação de expansão antes de poder desativar um nó de armazenamento existente.
- Se o nó de storage for desconectado ao desativá-lo, o sistema deverá reconstruir os dados usando dados dos nós de storage conectados, o que pode resultar em perda de dados.
- Quando você remove um nó de armazenamento, grandes volumes de dados de objeto devem ser transferidos pela rede. Embora essas transferências não devam afetar as operações normais do sistema, elas podem ter um impacto na quantidade total de largura de banda de rede consumida pelo sistema StorageGRID.
- As tarefas associadas à desativação do nó de storage recebem uma prioridade menor do que as tarefas associadas às operações normais do sistema. Isso significa que a desativação não interfere nas operações normais do sistema StorageGRID e não precisa ser programada para um período de inatividade do sistema. Como a desativação é realizada em segundo plano, é difícil estimar quanto tempo o processo levará para ser concluído. Em geral, a desativação termina mais rapidamente quando o sistema está silencioso ou se apenas um nó de armazenamento está sendo removido de cada vez.
- Pode levar dias ou semanas para desativar um nó de storage. Planeie este procedimento em conformidade. Embora o processo de desativação seja projetado para não impactar as operações do sistema, ele pode limitar outros procedimentos. Em geral, você deve executar quaisquer atualizações ou expansões planejadas do sistema antes de remover nós de grade.
- Os procedimentos de desativação que envolvem nós de storage podem ser pausados durante determinados estágios para permitir que outros procedimentos de manutenção sejam executados, se necessário, e retomados assim que forem concluídos.
- Não é possível executar operações de reparo de dados em nenhum nó de grade quando uma tarefa de desativação está em execução.
- Você não deve fazer alterações na política de ILM enquanto um nó de storage estiver sendo desativado.
- Quando você remove um nó de storage, os dados no nó são migrados para outros nós de grade; no entanto, esses dados não são completamente removidos do nó de grade desativado. Para remover dados de forma permanente e segura, você deve limpar as unidades do nó de grade desativado após o procedimento de desativação ser concluído.
- Quando você desativa um nó de armazenamento, os seguintes alertas e alarmes podem ser enviados e você pode receber notificações de e-mail e SNMP relacionadas:
 - **Não é possível se comunicar com o alerta node.** Esse alerta é acionado quando você desativa um nó de armazenamento que inclui o serviço ADC. O alerta é resolvido quando a operação de desativação é concluída.
 - Alarme VSTU (Estado da verificação do objeto). Este alarme de nível de aviso indica que o nó de armazenamento está a entrar no modo de manutenção durante o processo de desativação.
 - Alarme CASA (Data Store Status). Esse alarme de nível principal indica que o banco de dados Cassandra está caindo porque os serviços pararam.

Informações relacionadas

[Restaure os dados do objeto para o volume de storage, se necessário](#)

Entenda o quórum de ADC

Talvez você não consiga desativar certos nós de armazenamento em um local de data

center se muito poucos serviços do controlador de domínio administrativo (ADC) permanecessem após a desativação. Esse serviço, que é encontrado em alguns nós de storage, mantém informações de topologia de grade e fornece serviços de configuração para a grade. O sistema StorageGRID requer que um quórum de serviços ADC esteja disponível em cada local e em todos os momentos.

Não é possível desativar um nó de armazenamento se a remoção do nó fizer com que o quórum de ADC deixe de ser atendido. Para satisfazer o quórum de ADC durante a desativação, um mínimo de três nós de armazenamento em cada local de data center deve ter o serviço ADC. Se um local de data center tiver mais de três nós de storage com o serviço ADC, uma maioria simples desses nós deve permanecer disponível após a desativação ($(0,5 * Storage\ Nodes\ with\ ADC) + 1$).

Por exemplo, suponha que um site de data center inclua atualmente seis nós de storage com serviços ADC e que você queira desativar três nós de storage. Devido ao requisito de quórum do ADC, você deve concluir dois procedimentos de desativação, como segue:

- No primeiro procedimento de desativação, você deve garantir que quatro nós de armazenamento com serviços ADC permaneçam disponíveis ($(0,5 * 6) - 1$). Isso significa que você só pode desativar dois nós de storage inicialmente.
- No segundo procedimento de desativação, você pode remover o terceiro nó de armazenamento porque o quórum de ADC agora requer apenas três serviços ADC para permanecer disponível ($(0,5 * 4) + 1$).

Se você precisar desativar um nó de armazenamento, mas não puder devido ao requisito de quórum de ADC, você deve adicionar um novo nó de armazenamento em uma expansão e especificar que ele deve ter um serviço ADC. Em seguida, você pode desativar o nó de storage existente.

Informações relacionadas

[Expanda sua grade](#)

Reveja a política de ILM e a configuração de armazenamento

Se você planeja desativar um nó de storage, deve revisar a política de ILM do sistema StorageGRID antes de iniciar o processo de desativação.

Durante a desativação, todos os dados de objetos são migrados do nó de storage desativado para outros nós de storage.



A política ILM que você tem *durante* a desativação será a usada *após* a desativação. Você deve garantir que essa política atenda aos requisitos de dados antes de iniciar a desativação e após a conclusão da desativação.

Deve rever as regras da política ILM ativa para garantir que o sistema StorageGRID continuará a ter capacidade suficiente do tipo correto e nos locais corretos para acomodar a desativação de um nó de armazenamento.

Considere o seguinte:

- Será possível que os serviços de avaliação ILM copiem dados de objetos de modo que as regras ILM sejam satisfeitas?
- O que acontece se um site ficar temporariamente indisponível enquanto a desativação estiver em andamento? Cópias adicionais podem ser feitas em um local alternativo?

- Como o processo de desativação afetará a distribuição final do conteúdo? Conforme descrito em [Consolide os nós de storage](#), você deve adicionar novos nós de storage antes de desativar os antigos. Se você adicionar um nó de storage de substituição maior após a desativação de um nó de storage menor, os nós de storage antigos poderão estar próximos da capacidade e o novo nó de storage quase não terá conteúdo. A maioria das operações de gravação para novos dados de objetos seria direcionada para o novo nó de storage, reduzindo a eficiência geral das operações do sistema.
- O sistema incluirá, em todos os momentos, nós de storage suficientes para satisfazer a política de ILM ativa?



Uma política de ILM que não pode ser satisfeita levará a backlogs e alarmes e pode interromper a operação do sistema StorageGRID.

Verifique se a topologia proposta que resultará do processo de desativação satisfaz a política de ILM, avaliando os fatores listados na tabela.

Área a avaliar	Notas
Capacidade disponível	Haverá capacidade de armazenamento suficiente para acomodar todos os dados de objetos armazenados no sistema StorageGRID, incluindo as cópias permanentes de dados de objetos atualmente armazenados no nó de armazenamento para serem desativados? Haverá capacidade suficiente para lidar com o crescimento esperado de dados de objetos armazenados por um intervalo de tempo razoável após a conclusão da desativação?
Localização do armazenamento	Se ainda houver capacidade suficiente no sistema StorageGRID como um todo, a capacidade nos locais certos está em conformidade com as regras de negócios do sistema StorageGRID?
Tipo de armazenamento	Haverá armazenamento suficiente do tipo apropriado após a conclusão da desativação? Por exemplo, as regras do ILM podem ditar que o conteúdo seja movido de um tipo de armazenamento para outro à medida que o conteúdo envelhece. Nesse caso, você deve garantir que o armazenamento suficiente do tipo apropriado esteja disponível na configuração final do sistema StorageGRID.

Informações relacionadas

[Gerenciar objetos com ILM](#)

[Expanda sua grade](#)

Desativar nós de storage desconetados

Você deve entender o que pode acontecer se você desativar um nó de armazenamento enquanto ele estiver desconetado (integridade é desconhecido ou administrativamente inativo).

Quando você desativa um nó de storage desconetado da grade, o StorageGRID usa dados de outros nós de storage para reconstruir os dados do objeto e os metadados que estavam no nó desconetado. Ele faz isso iniciando automaticamente os trabalhos de reparo de dados no final do processo de desativação.

Antes de desativar um nó de storage desconetado, esteja ciente do seguinte:

- Você nunca deve desativar um nó desconetado, a menos que tenha certeza de que ele não pode ser colocado on-line ou recuperado.



Não execute este procedimento se você acredita que pode ser possível recuperar dados de objeto do nó. Em vez disso, entre em Contato com o suporte técnico para determinar se a recuperação do nó é possível.

- Se um nó de armazenamento desconetado contiver a única cópia de um objeto, esse objeto será perdido quando você desativar o nó. As tarefas de reparo de dados só podem reconstruir e recuperar objetos se houver pelo menos uma cópia replicada ou fragmentos codificados de apagamento suficientes nos nós de storage que estão atualmente conectados.
- Quando você desativa um nó de storage desconetado, o procedimento de desativação é concluído com relativa rapidez. No entanto, os trabalhos de reparação de dados podem demorar dias ou semanas a ser executados e não são monitorizados pelo procedimento de desativação. Você deve monitorar manualmente esses trabalhos e reiniciá-los conforme necessário. [Verifique os trabalhos de reparação de dados](#) Consulte .
- Se você desativar mais de um nó de storage desconetado de cada vez, poderá ocorrer perda de dados. O sistema pode não conseguir reconstruir dados se houver poucas cópias de dados de objetos, metadados ou fragmentos codificados por apagamento permanecerem disponíveis.



Se você tiver mais de um nó de armazenamento desconetado que não possa recuperar, entre em Contato com o suporte técnico para determinar o melhor curso de ação.

Consolide os nós de storage

Você pode consolidar os nós de storage para reduzir a contagem de nós de storage para um local ou implantação, aumentando a capacidade de storage.

Ao consolidar os nós de storage, você expande o sistema StorageGRID para adicionar nós de storage de capacidade novos e maiores e, em seguida, desativar os nós de storage de capacidade antigos e menores. Durante o procedimento de desativação, os objetos são migrados dos nós de armazenamento antigos para os novos nós de armazenamento.



Se você estiver consolidando dispositivos mais antigos e menores com novos modelos ou dispositivos de maior capacidade, muitos usarão o recurso de clone de nó ou o procedimento de clone de nó e o procedimento de desativação se não estiver fazendo uma substituição individual.

Por exemplo, você pode adicionar dois nós de storage de capacidade novos e maiores para substituir três nós de storage mais antigos. Primeiro, você usaria o procedimento de expansão para adicionar os dois nós de storage novos e maiores e, em seguida, usaria o procedimento de desativação para remover os três nós de storage de capacidade antigos e menores.

Ao adicionar nova capacidade antes de remover nós de storage existentes, você garante uma distribuição mais equilibrada dos dados pelo sistema StorageGRID. Você também reduz a possibilidade de que um nó de armazenamento existente possa ser empurrado para além do nível de marca d'água de armazenamento.

Informações relacionadas

[Expanda sua grade](#)

Desativar vários nós de storage

Se você precisar remover mais de um nó de storage, poderá desativá-los sequencialmente ou em paralelo.

- Se você desativar os nós de storage sequencialmente, deverá aguardar que o primeiro nó de storage conclua a desativação antes de começar a desativar o próximo nó de storage.
- Se você desativar os nós de storage em paralelo, os nós de storage processarão simultaneamente as tarefas de desativação de todos os nós de storage que estão sendo desativados. Isso pode resultar em uma situação em que todas as cópias permanentes de um arquivo são marcadas como "somente reativas", desativando temporariamente a exclusão em grades onde essa funcionalidade está ativada.

Verifique os trabalhos de reparação de dados

Antes de desativar um nó de grade, você deve confirmar que nenhum trabalho de reparo de dados está ativo. Se alguma reparação tiver falhado, tem de as reiniciar e permitir que sejam concluídas antes de executar o procedimento de desativação.

Se precisar desativar um nó de armazenamento desconetado, você também concluirá estes passos após a conclusão do procedimento de desativação para garantir que o trabalho de reparo de dados foi concluído com êxito. Você deve garantir que todos os fragmentos codificados de apagamento que estavam no nó removido foram restaurados com sucesso.

Essas etapas se aplicam somente a sistemas que tenham objetos codificados por apagamento.

1. Faça login no nó de administração principal:

- a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

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

- 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.

2. Verifique se existem reparações em curso: `repair-data show-ec-repair-status`

- Se nunca tiver executado um trabalho de reparação de dados, a saída é `No job found`. Não é necessário reiniciar quaisquer trabalhos de reparação.
- Se o trabalho de reparação de dados tiver sido executado anteriormente ou estiver em execução atualmente, a saída lista as informações para a reparação. Cada reparação tem um ID de reparação exclusivo. Vá para a próxima etapa.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status
```

```
Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired  
Retry Repair
```

```
=====
```

Repair ID	Scope	Start Time	End Time	State	Est/Affected Bytes	Repaired	Retry Repair
949283	DC1-S-99-10 (Volumes: 1,2)	2016-11-30T15:27:06.9		Success	17359	17359	No
949292	DC1-S-99-10 (Volumes: 1,2)	2016-11-30T15:37:06.9		Failure	17359	0	Yes
949294	DC1-S-99-10 (Volumes: 1,2)	2016-11-30T15:47:06.9		Failure	17359	0	Yes
949299	DC1-S-99-10 (Volumes: 1,2)	2016-11-30T15:57:06.9		Failure	17359	0	Yes

3. Se o Estado para todas as reparações for `Success`, não é necessário reiniciar quaisquer trabalhos de reparação.
4. Se o estado de qualquer reparação for `Failure`, tem de reiniciar a reparação.
 - a. Obtenha a ID de reparação para a reparação com falha a partir da saída.
 - b. Executar o `repair-data start-ec-node-repair` comando.

Utilize a `--repair-id` opção para especificar a ID de reparação. Por exemplo, se você quiser tentar novamente um reparo com a ID de reparo 949292, execute este comando: `repair-data start-ec-node-repair --repair-id 949292`

- c. Continuar a acompanhar o estado das reparações de dados CE até que o Estado para todas as reparações seja `Success`de` .

Reúna os materiais necessários

Antes de executar uma desativação de um nó de grade, você deve obter as seguintes informações.

Item	Notas
Arquivo do pacote de recuperação <code>.zip</code>	Tem de Baixe o mais recente pacote de recuperação .zip (<code>`sgws-recovery-package-id-revision.zip`</code> arquivar). Você pode usar o arquivo Pacote de recuperação para restaurar o sistema se ocorrer uma falha.
<code>Passwords.txt</code> ficheiro	Este arquivo contém as senhas necessárias para acessar os nós de grade na linha de comando e está incluído no Pacote de recuperação.
Frase-passe do aprovisionamento	A frase-passe é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no <code>Passwords.txt</code> arquivo.

Item	Notas
Descrição da topologia do sistema StorageGRID antes da desativação	Se disponível, obtenha qualquer documentação que descreva a topologia atual do sistema.

Informações relacionadas

[Requisitos do navegador da Web](#)

Acesse a página **Decommission Nodes**

Quando você acessa a página **Decommission Nodes** no Grid Manager, você pode ver rapidamente quais nós podem ser desativados.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão **Manutenção** ou **Acesso root**.

Passos

1. Selecione **MAINTENANCE > Tasks > Decommission**.
2. Selecione **Decommission Nodes**.

A página **Decommission Nodes** (nós de desintegração) é exibida. Nesta página, você pode:

- Determine quais nós de grade podem ser desativados atualmente.
- Veja a integridade de todos os nós de grade
- Classifique a lista em ordem crescente ou decrescente por **Nome**, **Site**, **tipo** ou **ADC**.
- Insira termos de pesquisa para encontrar rapidamente nós específicos. Por exemplo, esta página mostra nós de grade em dois data centers. A coluna **Decommission possible** (Descompactar possível) indica que você pode desativar o nó de gateway, um dos cinco nós de armazenamento e o nó de administração não primário.

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.



Grid Nodes

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
DC1-ARC1	Data Center 1	Archive Node	-		No, Archive Nodes decommissioning is not supported.
<input type="checkbox"/> DC1-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No		
<input type="checkbox"/> DC2-ADM1	Data Center 2	Admin Node	-		
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.

3. Revise a coluna **Decommission possible** para cada nó que você deseja desativar.

Se um nó de grade pode ser desativado, essa coluna inclui uma marca de seleção verde e a coluna mais à esquerda inclui uma caixa de seleção. Se um nó não puder ser desativado, essa coluna descreve o problema. Se houver mais de um motivo pelo qual um nó não pode ser desativado, o motivo mais crítico será exibido.

Desativar possível motivo	Descrição	Passos para resolver
Não, a desativação do tipo de nó não é suportada.	Não é possível desativar o nó de administração principal ou um nó de arquivo.	Nenhum.

Desativar possível motivo	Descrição	Passos para resolver
<p>Não, pelo menos um nó de grade está desconetado.</p> <p>Nota: esta mensagem é mostrada apenas para nós de grade conetados.</p>	<p>Você não pode desativar um nó de grade conetado se qualquer nó de grade estiver desconetado.</p> <p>A coluna Saúde inclui um destes ícones para nós de grade que estão desconetados:</p> <ul style="list-style-type: none"> •  (Cinza): Administrativamente para baixo •  (Azul): Desconhecido 	<p>Vá para etapa que lista as opções de procedimento de desativação.</p>
<p>Não, um ou mais nós necessários estão atualmente desconetados e devem ser recuperados.</p> <p>Nota: esta mensagem é mostrada apenas para nós de grade desconetados.</p>	<p>Você não pode desativar um nó de grade desconetado se um ou mais nós necessários também forem desconetados (por exemplo, um nó de armazenamento que é necessário para o quórum de ADC).</p>	<ol style="list-style-type: none"> a. Reveja as mensagens possíveis de desintegração para todos os nós desconetados. b. Determine quais nós não podem ser desativados porque são necessários. <ul style="list-style-type: none"> ◦ Se a integridade de um nó necessário estiver administrativamente para baixo, coloque o nó novamente online. ◦ Se a integridade de um nó necessário for desconhecido, execute um procedimento de recuperação de nó para recuperar o nó necessário.
<p>Não, membro do(s) grupo(s) HA: X. Antes de desativar esse nó, você deve removê-lo de todos os grupos de HA.</p>	<p>Não é possível desativar um nó de administrador ou um nó de gateway se uma interface de nó pertencer a um grupo de alta disponibilidade (HA).</p>	<p>Edite o grupo de HA para remover a interface do nó ou remover todo o grupo de HA. Consulte as instruções para administrar o StorageGRID.</p>
<p>Não, o local x requer um mínimo de n nós de armazenamento com serviços ADC.</p>	<p>Somente nós de storage. Você não pode desativar um nó de storage se nós insuficientes permanecessem no local para oferecer suporte aos requisitos de quórum de ADC.</p>	<p>Execute uma expansão. Adicione um novo nó de armazenamento ao site e especifique que ele deve ter um serviço ADC. Consulte informações sobre o quórum ADC.</p>

Desativar possível motivo	Descrição	Passos para resolver
<p>Não, um ou mais perfis de codificação de apagamento precisam de pelo menos n nós de storage. Se o perfil não for usado em uma regra ILM, você poderá desativá-lo.</p>	<p>Somente nós de storage. Você não pode desativar um nó de storage a menos que haja nós suficientes para os perfis de codificação de apagamento existentes.</p> <p>Por exemplo, se existir um perfil de codificação de apagamento para 4 codificação de apagamento a mais de 2 anos, pelo menos 6 nós de storage devem permanecer.</p>	<p>Para cada perfil de codificação de apagamento afetado, execute uma das seguintes etapas, com base em como o perfil está sendo usado:</p> <ul style="list-style-type: none"> • Usado na política ILM ativa: Execute uma expansão. Adicione nós de storage novos suficientes para permitir que a codificação de apagamento continue. Consulte as instruções para expandir o StorageGRID. • Usado em uma regra ILM, mas não na política ILM ativa: Edite ou exclua a regra e desative o perfil de codificação de apagamento. • Não usado em nenhuma regra ILM: Desative o perfil de codificação de apagamento. <p>Observação: uma mensagem de erro aparece se você tentar desativar um perfil de codificação de apagamento e os dados de objeto ainda estiverem associados ao perfil. Talvez seja necessário esperar várias semanas antes de tentar novamente o processo de desativação.</p> <p>Saiba mais sobre como desativar um perfil de codificação de apagamento nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.</p>

4. se a desativação for possível para o nó, determine qual procedimento você precisa executar:

Se sua grade inclui...	Ir para...
Quaisquer nós de grade desconetados	Desativar nós de grade desconetados
Somente nós de grade conetados	Desativar os nós de grade conetados

Informações relacionadas

[Verifique os trabalhos de reparação de dados](#)

[Entenda o quórum de ADC](#)

[Gerenciar objetos com ILM](#)

[Expanda sua grade](#)

[Administrar o StorageGRID](#)

Desativar nós de grade desconetados

Talvez seja necessário desativar um nó que não esteja conetado à grade no momento (aquele cuja Saúde é desconhecida ou administrativamente inativa).

O que você vai precisar


- Você entende os requisitos e [considerações para a desativação de nós de grade](#).
- Você obteve todos os itens pré-requisitos.
- Você garantiu que nenhum trabalho de reparo de dados está ativo. [Verifique os trabalhos de reparação de dados](#)Consulte .
- Você confirmou que a recuperação do nó de storage não está em andamento em nenhum lugar da grade. Se estiver, você deve esperar até que qualquer reconstrução do Cassandra executada como parte da recuperação esteja concluída. Você pode então prosseguir com a desativação.
- Você garantiu que outros procedimentos de manutenção não serão executados enquanto o procedimento de desativação do nó estiver em execução, a menos que o procedimento de desativação do nó esteja pausado.
- A coluna **Decommission possible** para o nó ou nós desconetados que você deseja desativar inclui uma marca de seleção verde.
- Você deve ter a senha de provisionamento.

Sobre esta tarefa

Você pode identificar nós desconetados procurando por ícones desconhecidos (azul) ou administrativamente para baixo (cinza) na coluna **Saúde**. No exemplo, o nó de storage chamado DC1-S4 é desconetado; todos os outros nós estão conetados.

Decommission Nodes



Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

 A grid node is disconnected (has a blue or gray health icon). Try to bring it back online or recover it. Data loss might occur if you decommission a node that is disconnected.

See the [Recovery and Maintenance Guide](#) for details. Contact Support if you cannot recover a node and do not want to decommission it.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the [Recovery and Maintenance Guide](#) to learn how to proceed.

Grid Nodes

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
DC1-ADM2	Data Center 1	Admin Node	-		No, at least one grid node is disconnected.
DC1-G1	Data Center 1	API Gateway Node	-		No, at least one grid node is disconnected.
DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No		

Passphrase

Provisioning
Passphrase

Start Decommission

Antes de desativar qualquer nó desconetado, observe o seguinte:

- Este procedimento destina-se principalmente à remoção de um único nó desconetado. Se sua grade contiver vários nós desconetados, o software exige que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.



Tenha muito cuidado ao desativar mais de um nó de grade desconetado de cada vez, especialmente se você estiver selecionando vários nós de storage desconetados.

- Se um nó desconetado não puder ser removido (por exemplo, um nó de armazenamento necessário para o quórum de ADC), nenhum outro nó desconetado poderá ser removido.

Antes de desativar um **nó de armazenamento** desconetado, observe o seguinte

- Você nunca deve desativar um nó de armazenamento desconetado, a menos que tenha certeza de que ele não pode ser colocado on-line ou recuperado.



Se você acredita que os dados do objeto ainda podem ser recuperados do nó, não execute este procedimento. Em vez disso, entre em Contato com o suporte técnico para determinar se a recuperação do nó é possível.

- Se você desativar mais de um nó de storage desconetado, poderá ocorrer perda de dados. O sistema pode não ser capaz de reconstruir dados se não houver cópias suficientes de objetos, fragmentos codificados para apagamento ou metadados de objetos permanecerem disponíveis.



Se você tiver mais de um nó de armazenamento desconetado que não possa recuperar, entre em Contato com o suporte técnico para determinar o melhor curso de ação.

- Quando você desativa um nó de storage desconetado, o StorageGRID inicia os trabalhos de reparo de dados no final do processo de desativação. Essas tarefas tentam reconstruir os dados do objeto e os metadados armazenados no nó desconetado.
- Quando você desativa um nó de storage desconetado, o procedimento de desativação é concluído com relativa rapidez. No entanto, os trabalhos de reparação de dados podem demorar dias ou semanas a ser executados e não são monitorizados pelo procedimento de desativação. Você deve monitorar manualmente esses trabalhos e reiniciá-los conforme necessário. [Verifique os trabalhos de reparação de dados](#) Consulte .
- Se você desativar um nó de armazenamento desconetado que contenha a única cópia de um objeto, o objeto será perdido. As tarefas de reparo de dados só podem reconstruir e recuperar objetos se houver pelo menos uma cópia replicada ou fragmentos codificados de apagamento suficientes nos nós de storage que estão atualmente conectados.

Antes de desativar um **Admin Node** ou **Gateway Node** desconetado, observe o seguinte:

- Ao desativar um nó Admin desconetado, você perderá os logs de auditoria desse nó; no entanto, esses logs também devem existir no nó Admin principal.
- Você pode desativar um Gateway Node com segurança enquanto ele estiver desconetado.

Passos

1. Tente colocar todos os nós de grade desconetados novamente on-line ou recuperá-los.

Consulte os procedimentos de recuperação para obter instruções.

2. Se você não conseguir recuperar um nó de grade desconetado e quiser desativá-lo enquanto ele estiver desconetado, marque a caixa de seleção desse nó.



Se sua grade contiver vários nós desconetados, o software exige que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.



Tenha muito cuidado ao escolher desativar mais de um nó de grade desconetado de cada vez, especialmente se você estiver selecionando vários nós de storage desconetados. Se você tiver mais de um nó de armazenamento desconetado que não possa recuperar, entre em Contato com o suporte técnico para determinar o melhor curso de ação.

3. Introduza a frase-passe de provisionamento.

O botão **Start Decommission** está ativado.

4. Clique em **Start Decommission**.

Um aviso é exibido, indicando que você selecionou um nó desconetado e que os dados do objeto serão perdidos se o nó tiver a única cópia de um objeto.

Warning

The selected nodes are disconnected (health is Unknown or Administratively Down). If you continue and the node has the only copy of an object, the object will be lost when the node is removed.

The following grid nodes have been selected for decommissioning and will be permanently removed from the StorageGRID Webscale system.

DC1-S4

Do you want to continue?

Cancel

OK

5. Revise a lista de nós e clique em **OK**.

O procedimento de desativação é iniciado e o progresso é exibido para cada nó. Durante o procedimento, um novo Pacote de recuperação é gerado contendo a alteração de configuração da grade.

Decommission Nodes

A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S4	Storage Node	<div style="width: 10%;"></div>	Prepare Task

Search

Pause Resume

6. Assim que o novo Pacote de recuperação estiver disponível, clique no link ou selecione **MANUTENÇÃO sistema Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o .zip arquivo.

Consulte as instruções para [Transferir o pacote de recuperação](#).



Baixe o pacote de recuperação o mais rápido possível para garantir que você possa recuperar sua grade se algo der errado durante o procedimento de desativação.



O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

7. Monitorize periodicamente a página de desativação para garantir que todos os nós selecionados sejam desativados com êxito.

Os nós de storage podem levar dias ou semanas para serem desativados. Quando todas as tarefas

estiverem concluídas, a lista de seleção de nós é reexibida com uma mensagem de sucesso. Se você tiver desativado um nó de armazenamento desconectado, uma mensagem de informações indicará que os trabalhos de reparo foram iniciados.

Decommission Nodes

The previous decommission procedure completed successfully.

i Repair jobs for replicated and erasure-coded data have been started. These jobs restore object data that might have been on any disconnected Storage Nodes. To monitor the progress of these jobs and restart them as needed, see the Decommissioning section of the Recovery and Maintenance Guide.

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, primary Admin Node decommissioning is not supported.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, Archive Nodes decommissioning is not supported.
<input type="checkbox"/> DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No	✓	✓
<input type="checkbox"/> DC2-ADM1	Data Center 2	Admin Node	-	✓	✓
DC2-S1	Data Center 2	Storage Node	Yes	✓	No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.

- Depois que os nós forem desligados automaticamente como parte do procedimento de desativação, remova quaisquer máquinas virtuais restantes ou outros recursos associados ao nó desativado.



Não execute esta etapa até que os nós sejam desligados automaticamente.

- Se você estiver desativando um nó de storage, monitore o status dos trabalhos de reparo **dados replicados** e **dados codificados por apagamento (EC)** que são iniciados automaticamente durante o processo de desativação.

Dados replicados

- Para determinar se as reparações estão concluídas:
 - a. Selecione **NODES > Storage Node a ser reparado > ILM**.
 - b. Reveja os atributos na seção avaliação. Quando os reparos estiverem concluídos, o atributo **aguardando - All** indica objetos 0D.
- Para monitorizar a reparação em mais detalhes:
 - a. Selecione **SUPPORT > Tools > Grid topology**.
 - b. Selecione **Grid > Storage Node a ser reparado > LDR > Data Store**.
 - c. Use uma combinação dos seguintes atributos para determinar, assim como possível, se as reparações replicadas estão concluídas.



As inconsistências do Cassandra podem estar presentes e as reparações falhadas não são rastreadas.

- * Tentativas de reparos (XRPA): **Use este atributo para rastrear o progresso de reparos replicados. Esse atributo aumenta cada vez que um nó de storage tenta reparar um objeto de alto risco. Quando este atributo não aumenta por um período superior ao período de digitalização atual (fornecido pelo atributo *período de digitalização — estimado), significa que a digitalização ILM não encontrou objetos de alto risco que precisam ser reparados em nenhum nó.**



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração ILM.

- **Período de digitalização — estimado (XSCM):** Use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Repairs tented** não aumentar durante um período superior ao período de digitalização atual, é provável que sejam efetuadas reparações replicadas. Note que o período de digitalização pode mudar. O atributo **período de digitalização — estimado (XSCM)** aplica-se a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico de atributos **período de digitalização — estimado** para a grade para determinar um período de tempo apropriado.
- Opcionalmente, para obter uma conclusão percentual estimada para o reparo replicado, adicione a `show-replicated-repair-status` opção ao comando `repair-data`.

```
repair-data show-replicated-repair-status
```



A `show-replicated-repair-status` opção está disponível para pré-visualização técnica no StorageGRID 11,6. Este recurso está em desenvolvimento e o valor retornado pode estar incorreto ou atrasado. Para determinar se uma reparação está concluída, utilize **aguardando – todos, tentativas de reparação (XRPA)** e **período de digitalização — estimado (XSCM)**, conforme descrito em [Monitorize as reparações](#).

Dados codificados para apagamento (EC)

Para monitorar o reparo de dados codificados por apagamento e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por apagamento:

- Selecione **SUPPORT > Tools > Metrics** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **EC Overview** na seção Grafana. Veja os painéis **Grid EC Job tempo estimado para conclusão** e **Grid EC Job percentage Completed**.

- Use este comando para ver o status de uma operação específica `repair-data`:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilize este comando para listar todas as reparações:

```
repair-data show-ec-repair-status
```

A saída lista informações, `repair ID` incluindo , para todas as reparações anteriores e atualmente em execução.

2. Se a saída mostrar que a operação de reparo falhou, use a `--repair-id` opção para tentar novamente a reparação.

Este comando tenta novamente um reparo de nó com falha, usando a ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente uma reparação de volume com falha, utilizando a ID de reparação 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Depois de terminar

Assim que os nós desconetados forem desativados e todos os trabalhos de reparo de dados tiverem sido concluídos, você poderá desativar todos os nós de grade conetados conforme necessário.

Em seguida, execute estas etapas depois de concluir o procedimento de desativação:


- Certifique-se de que as unidades do nó de grade desativado estão limpas. Utilize uma ferramenta ou serviço de limpeza de dados disponíveis no mercado para remover dados das unidades de forma permanente e segura.
- Se você desativou um nó de dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o Instalador de dispositivos StorageGRID para limpar a configuração do servidor de gerenciamento de chaves (limpar KMS). Você deve limpar a configuração do KMS se quiser adicionar o dispositivo a outra grade.
 - [Aparelhos de serviços SG100 e SG1000](#)
 - [SG5600 dispositivos de armazenamento](#)
 - [SG5700 dispositivos de armazenamento](#)
 - [SG6000 dispositivos de armazenamento](#)





Informações relacionadas

[Procedimentos de recuperação do nó de grade](#)

Desativar os nós de grade conectados

Você pode desativar e remover permanentemente nós que estão conectados à grade.

- Você deve entender os requisitos e [considerações para a desativação de nós de grade](#).
- Você deve ter reunido todos os materiais necessários.
- Tem de ter assegurado que não estão ativos trabalhos de reparação de dados.
- Você deve ter confirmado que a recuperação do nó de storage não está em andamento em nenhum lugar da grade. Se estiver, você deve esperar até que qualquer reconstrução do Cassandra executada como parte da recuperação esteja concluída. Você pode então prosseguir com a desativação.
- Você deve ter garantido que outros procedimentos de manutenção não serão executados enquanto o procedimento de desativação do nó estiver em execução, a menos que o procedimento de desativação do nó esteja pausado.
- Você deve ter a senha de provisionamento.
- Os nós de grade estão conectados.
- A coluna **Decmission possible** para o nó ou nós que você deseja desativar deve incluir uma marca de seleção verde.
- Todos os nós da grade devem ter a saúde normal (verde) . Se você vir um desses ícones na coluna **Saúde**, tente resolver o problema:

Ícone	Cor	Gravidade
	Amarelo	Aviso
	Laranja claro	Menor
	Laranja escuro	Maior
	Vermelho	Crítico

- Se você desativou anteriormente um nó de storage desconectado, todos os trabalhos de reparo de dados foram concluídos com êxito. [Verifique os trabalhos de reparação de dados](#)Consulte .



Não remova a máquina virtual de um nó de grade ou outros recursos até que seja instruído a fazê-lo neste procedimento.

1. Na página Decommission Nodes, marque a caixa de seleção para cada nó de grade que deseja desativar.
2. Introduza a frase-passe de provisionamento.

O botão **Start Decommission** está ativado.

3. Clique em **Start Decommission**.

É apresentada uma caixa de diálogo de confirmação.

Info

The following grid nodes have been selected for decommissioning and will be permanently removed from the StorageGRID Webscale system.

DC1-S5

Do you want to continue?

Cancel

OK

4. Revise a lista de nós selecionados e clique em **OK**.

O procedimento de desativação do nó é iniciado e o progresso é exibido para cada nó. Durante o procedimento, um novo pacote de recuperação é gerado para mostrar a alteração da configuração da grade.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S5	Storage Node	<div style="width: 10%;"></div>	Prepare Task

Search

Pause Resume



Não coloque um nó de armazenamento offline após o início do procedimento de desativação. Alterar o estado pode resultar em algum conteúdo não ser copiado para outros locais.

5. Assim que o novo Pacote de recuperação estiver disponível, clique no link ou selecione **MANUTENÇÃO sistema Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o .zip arquivo.

Consulte as instruções para [Transferir o pacote de recuperação](#).



Baixe o pacote de recuperação o mais rápido possível para garantir que você possa recuperar sua grade se algo der errado durante o procedimento de desativação.

6. Monitore periodicamente a página Decommission Nodes para garantir que todos os nós selecionados sejam desativados com êxito.

Os nós de storage podem levar dias ou semanas para serem desativados. Quando todas as tarefas estiverem concluídas, a lista de seleção de nós é reexibida com uma mensagem de sucesso.

Decommission Nodes

The previous decommission procedure completed successfully.

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, primary Admin Node decommissioning is not supported.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, Archive Nodes decommissioning is not supported.
<input type="checkbox"/> DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No	✓	✓
<input type="checkbox"/> DC2-ADM1	Data Center 2	Admin Node	-	✓	✓
DC2-S1	Data Center 2	Storage Node	Yes	✓	No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.

7. Siga o passo apropriado para a sua plataforma. Por exemplo:

- *** Linux***: Você pode querer desanexar os volumes e excluir os arquivos de configuração de nó criados durante a instalação.
- **VMware**: Você pode querer usar a opção "Excluir do disco" do vCenter para excluir a máquina virtual. Você também pode precisar excluir quaisquer discos de dados que sejam independentes da máquina virtual.
- **StorageGRID Appliance**: O nó appliance reverte automaticamente para um estado não implantado, onde você pode acessar o Instalador de dispositivos StorageGRID. Pode desligar o aparelho ou adicioná-lo a outro sistema StorageGRID.

Siga estas etapas depois de concluir o procedimento de desativação do nó:

- Certifique-se de que as unidades do nó de grade desativado estão limpas. Utilize uma ferramenta ou serviço de limpeza de dados disponíveis no mercado para remover dados das unidades de forma permanente e segura.
- Se você desativou um nó de dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o Instalador de dispositivos StorageGRID para limpar a configuração do servidor de gerenciamento de chaves (limpar KMS). Você deve limpar a configuração do KMS se quiser usar o dispositivo em outra grade.

[Aparelhos de serviços SG100 e SG1000](#)

[SG5600 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG6000 dispositivos de armazenamento](#)

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

Pausar e retomar o processo de desativação dos nós de storage

Se precisar executar um segundo procedimento de manutenção, você pode pausar o procedimento de desativação de um nó de armazenamento durante determinadas etapas. Depois que o outro procedimento for concluído, você pode retomar a desativação.



O botão **Pausa** é ativado somente quando os estágios de avaliação ILM ou desativação de dados codificados por apagamento forem alcançados; no entanto, a avaliação ILM (migração de dados) continuará a ser executada em segundo plano.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.

Passos

1. Selecione **MAINTENANCE > Tasks > Decommission**.

A página Decommission é exibida.

2. Selecione **Decommission Nodes**.


A página Decommission Nodes (nós de desintegração) é exibida. Quando o procedimento de desativação atinge uma das seguintes etapas, o botão **Pausa** é ativado.


- Avaliando o ILM
- Desativação de dados codificados de apagamento

3. Selecione **Pausa** para suspender o procedimento.

O estágio atual é pausado e o botão **Resume** está ativado.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

 Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S5	Storage Node	<div style="width: 100%; height: 10px; background-color: orange;"></div>	Evaluating ILM

4. Depois que o outro procedimento de manutenção estiver concluído, selecione **Resume** para prosseguir com a desativação.

Solucionar problemas de desativação do nó

Se o procedimento de desativação do nó parar por causa de um erro, você pode executar etapas específicas para solucionar o problema.

O que você vai precisar

Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

Se você desligar o nó da grade sendo desativado, a tarefa será interrompida até que o nó da grade seja reiniciado. O nó da grade deve estar online.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Na árvore Grid Topology, expanda cada entrada Storage Node e verifique se os serviços DDS e LDR estão ambos online.

Para realizar a desativação do nó de storage, todos os nós e todos os serviços precisam estar íntegros no início de uma desativação do nó/local on-line.

3. Para exibir as tarefas de grade ativa, selecione **nó de administração principal CMN tarefas de grade Visão geral**.
4. Verifique o estado da tarefa de desativação da grelha.
 - a. Se o status da tarefa de grade de desativação indicar um problema ao salvar pacotes de tarefas de grade, selecione **nó Admin primário CMN Eventos Visão geral**
 - b. Verifique o número de relés de auditoria disponíveis.

Se o atributo Available Audit Relay for um ou mais, o serviço CMN estará conectado a pelo menos um serviço ADC. Os serviços ADC atuam como relés de Auditoria.

O serviço CMN deve estar conectado a pelo menos um serviço ADC e a maioria (50% mais um) dos

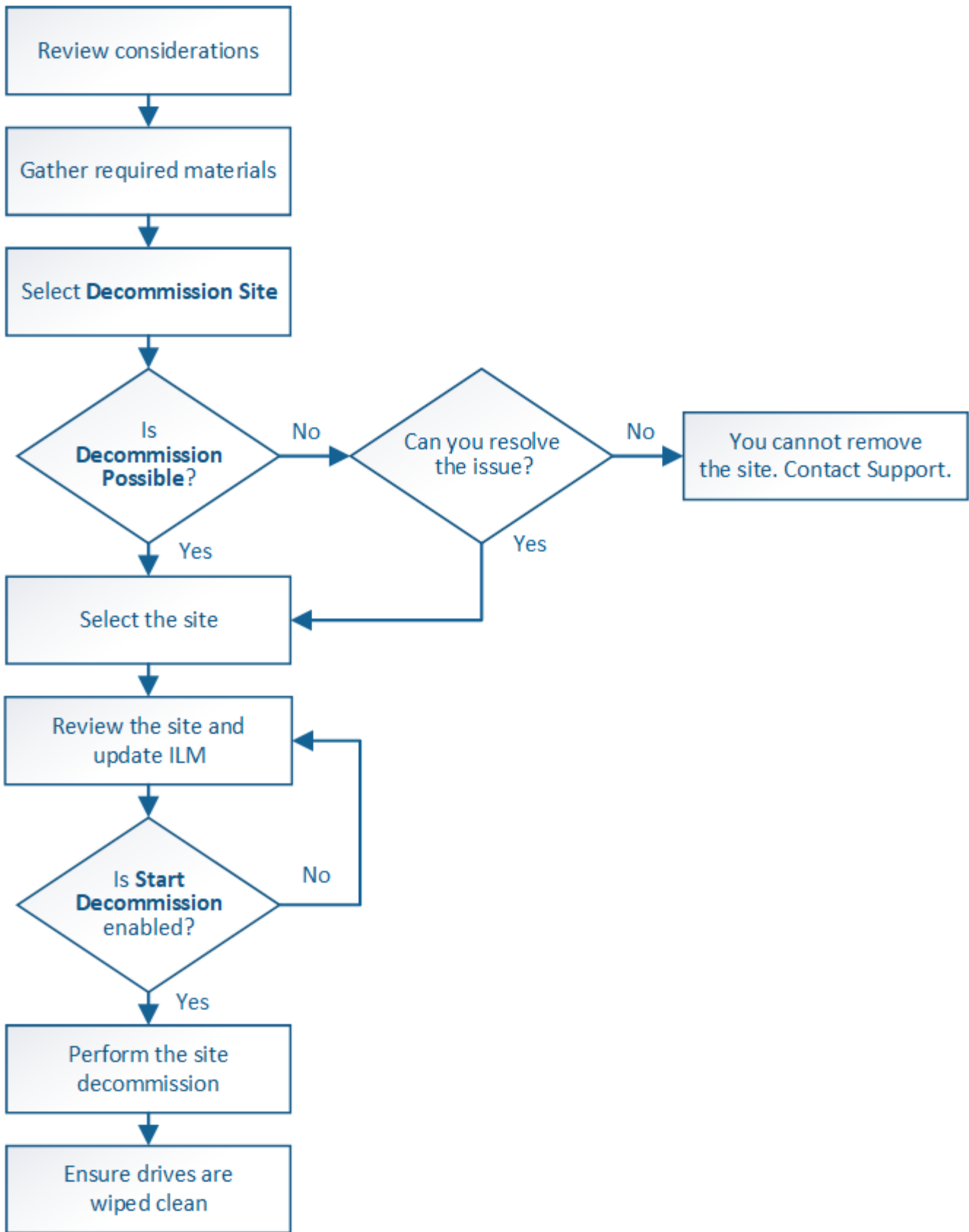
serviços ADC do sistema StorageGRID deve estar disponível para que uma tarefa de grade passe de um estágio de desativação para outro e termine.

- a. Se o serviço CMN não estiver conectado a serviços ADC suficientes, verifique se os nós de storage estão online e verifique a conectividade de rede entre o nó de administração principal e os nós de storage.

Desativação do site

Talvez seja necessário remover um site de data center do sistema StorageGRID. Para remover um site, você deve desativá-lo.

O fluxograma mostra as etapas de alto nível para a desativação de um local.



Considerações para remover um site

Antes de usar o procedimento de desativação do site para remover um site, você deve revisar as considerações.

O que acontece quando você desativa um site

Ao desativar um site, o StorageGRID remove permanentemente todos os nós do site e do próprio site do sistema StorageGRID.

Quando o procedimento de desativação do local estiver concluído:

- Você não pode mais usar o StorageGRID para visualizar ou acessar o site ou qualquer um dos nós no site.
- Você não pode mais usar pools de storage ou perfis de codificação de apagamento que se referissem ao site. Quando o StorageGRID descompacta um site, ele remove automaticamente esses pools de armazenamento e desativa esses perfis de codificação de apagamento.

Diferenças entre os procedimentos de desativação do local conectado e do local desconetado

Você pode usar o procedimento de desativação do site para remover um site no qual todos os nós estão conectados ao StorageGRID (chamado de desativação do site conectado) ou para remover um site no qual todos os nós são desconetados do StorageGRID (chamado de desativação do site desconetado). Antes de começar, você deve entender as diferenças entre esses procedimentos.



Se um site contiver uma mistura de nós conectados (🟢) e desconetados (🌑 ou 🌐), você deverá colocar todos os nós offline novamente online.

- Uma desativação do site conectado permite remover um site operacional do sistema StorageGRID. Por exemplo, você pode executar uma desativação do site conectado para remover um site funcional, mas não mais necessário.
- Quando o StorageGRID remove um site conectado, ele usa o ILM para gerenciar os dados do objeto no site. Antes de poder iniciar uma desativação do site ligado, tem de remover o site de todas as regras ILM e ativar uma nova política ILM. Os processos de ILM para migrar dados de objeto e os processos internos para remover um local podem ocorrer ao mesmo tempo, mas a prática recomendada é permitir que as etapas de ILM sejam concluídas antes de iniciar o procedimento de desativação real.
- Uma desativação de site desconetada permite remover um site com falha do sistema StorageGRID. Por exemplo, você pode executar uma desativação do local desconetada para remover um local que foi destruído por um incêndio ou inundação.

Quando o StorageGRID remove um local desconetado, ele considera todos os nós irrecuperáveis e não tenta preservar os dados. No entanto, antes de poder iniciar uma desativação do site desligada, tem de remover o site de todas as regras ILM e ativar uma nova política ILM.









Antes de executar um procedimento de desativação do local desconetado, você deve entrar em Contato com seu representante da conta do NetApp. O NetApp revisará seus requisitos antes de ativar todas as etapas no assistente do site de desintegração. Você não deve tentar uma desativação de site desconetada se você acredita que pode ser possível recuperar o site ou recuperar dados de objeto do site.

Requisitos gerais para remover um local conectado ou desconetado

Antes de remover um local conectado ou desconetado, você deve estar ciente dos seguintes requisitos:

- Não é possível desativar um site que inclua o nó de administração principal.
- Não é possível desativar um site que inclua um nó de arquivo.

- Não é possível desativar um local se algum dos nós tiver uma interface que pertença a um grupo de alta disponibilidade (HA). Você deve editar o grupo de HA para remover a interface do nó ou remover todo o grupo de HA.
- Não é possível desativar um local se ele contiver uma mistura de  nós conectados () e desconectados ( ou ).
- Não é possível desativar um local se qualquer nó em qualquer outro local estiver desconectado ( ou ).
- Não é possível iniciar o procedimento de desativação do local se uma operação de reparação ec-node estiver em curso. [Verifique os trabalhos de reparação de dados](#) Consulte para rastrear reparos de dados codificados por apagamento.
- Enquanto o procedimento de desativação do site está em execução:
 - Você não pode criar regras ILM que se referem ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para se referir ao site.
 - Não é possível executar outros procedimentos de manutenção, como expansão ou atualização.



Se precisar executar outro procedimento de manutenção durante a desativação de um site conectado, você pode [Interrompa o procedimento enquanto os nós de storage estão sendo removidos](#). O botão **Pausa** é ativado somente quando os estágios de avaliação ILM ou desativação de dados codificados por apagamento forem alcançados; no entanto, a avaliação ILM (migração de dados) continuará a ser executada em segundo plano. Depois de concluído o segundo procedimento de manutenção, pode retomar a desativação.

- Se você precisar recuperar qualquer nó depois de iniciar o procedimento de desativação do site, entre em Contato com o suporte.
- Você não pode desativar mais de um local de cada vez.
- Se o site incluir um ou mais nós de administração e o logon único (SSO) estiver ativado para o seu sistema StorageGRID, você deverá remover todas as confianças de partes confiáveis para o site dos Serviços de Federação do Active Directory (AD FS).

Requisitos para o gerenciamento do ciclo de vida das informações (ILM)

Como parte da remoção de um site, você deve atualizar sua configuração ILM. O assistente do Decommission Site orienta você por várias etapas de pré-requisitos para garantir o seguinte:

- O site não é referido pela política ILM ativa. Se for, você deve criar e ativar uma nova política ILM com novas regras ILM.
- Não existe nenhuma política proposta de ILM. Se você tem uma política proposta, você deve excluí-la.
- Nenhuma regra de ILM se refere ao site, mesmo que essas regras não sejam usadas na política ativa ou proposta. Você deve excluir ou editar todas as regras que se referem ao site.

Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa todos os sites.



Antes de remover um site, talvez seja necessário criar novas regras ILM e ativar uma nova política ILM. Essas instruções assumem que você tem um bom entendimento de como o ILM funciona e que você está familiarizado com a criação de pools de armazenamento, perfis de codificação de apagamento, regras do ILM e a simulação e ativação de uma política de ILM. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Gerenciar objetos com ILM

Considerações para os dados do objeto em um local conectado

Se você estiver executando uma desativação do site conectado, você deve decidir o que fazer com os dados de objeto existentes no site quando criar novas regras ILM e uma nova política ILM. Você pode fazer um ou ambos os seguintes procedimentos:

- Mova os dados de objetos do site selecionado para um ou mais sites na grade.

Exemplo para mover dados: Suponha que você queira desativar um site em Raleigh porque adicionou um novo site em Sunnyvale. Neste exemplo, você deseja mover todos os dados de objeto do site antigo para o novo site. Antes de atualizar suas regras de ILM e a política de ILM, você deve revisar a capacidade em ambos os sites. Você precisa garantir que o local de Sunnyvale tenha capacidade suficiente para acomodar os dados de objeto do local de Raleigh e que a capacidade adequada permaneça em Sunnyvale para crescimento futuro.



Para garantir que a capacidade adequada esteja disponível, talvez seja necessário adicionar volumes de storage ou nós de storage a um local existente ou adicionar um novo local antes de executar este procedimento. Consulte as instruções para expandir um sistema StorageGRID.

- Excluir cópias de objetos do site selecionado.

Exemplo para excluir dados: Suponha que você use atualmente uma regra ILM de 3 cópias para replicar dados de objetos em três sites. Antes de desativar um site, você pode criar uma regra ILM equivalente a 2 cópias para armazenar dados em apenas dois sites. Quando você ativa uma nova política de ILM que usa a regra de 2 cópias, o StorageGRID exclui as cópias do terceiro site porque elas não atendem mais aos requisitos de ILM. No entanto, os dados do objeto ainda serão protegidos e a capacidade dos dois locais restantes permanecerá a mesma.



Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Requisitos adicionais para uma desativação do local conectado

Antes que o StorageGRID possa remover um site conectado, você deve garantir o seguinte:

- Todos os nós do seu sistema StorageGRID devem ter um estado de conexão **conectado** (✓); no entanto, os nós podem ter alertas ativos.



Você pode concluir as etapas 1-4 do assistente Decommission Site se um ou mais nós forem desconetados. No entanto, não é possível concluir a Etapa 5 do assistente, que inicia o processo de desativação, a menos que todos os nós estejam conectados.

- Se o site que você pretende remover contiver um nó de gateway ou um nó de administrador que seja usado para balanceamento de carga, talvez seja necessário executar um procedimento de expansão para adicionar um novo nó equivalente em outro local. Certifique-se de que os clientes podem se conectar ao nó de substituição antes de iniciar o procedimento de desativação do site.
- Se o site que você pretende remover contiver qualquer nó de gateway ou nós de administrador que estejam em um grupo de alta disponibilidade (HA), você poderá concluir as etapas 1-4 do assistente Decommission Site. No entanto, não é possível concluir a Etapa 5 do assistente, que inicia o processo de desativação, até remover esses nós de todos os grupos de HA. Se os clientes existentes se conectarem a um grupo de HA que inclua nós do site, você deverá garantir que eles possam continuar se conectando ao StorageGRID após a remoção do site.
- Se os clientes se conectarem diretamente aos nós de storage no local que você está planejando remover, você deverá garantir que eles possam se conectar aos nós de storage em outros locais antes de iniciar o procedimento de desativação do site.
- Você deve fornecer espaço suficiente nos locais restantes para acomodar quaisquer dados de objeto que serão movidos devido a alterações na política ILM ativa. Em alguns casos, talvez seja necessário expandir o sistema StorageGRID adicionando nós de storage, volumes de storage ou novos sites antes de concluir a desativação de um site conectado.
- Você deve permitir tempo adequado para que o procedimento de desativação seja concluído. Os processos de ILM da StorageGRID podem levar dias, semanas ou até meses para mover ou excluir dados de objetos do site antes que o site possa ser desativado.



A migração ou exclusão de dados de objetos de um local pode levar dias, semanas ou até meses, dependendo da quantidade de dados no local, da carga no sistema, das latências de rede e da natureza das mudanças necessárias no ILM.

- Sempre que possível, você deve completar os passos 1-4 do assistente Decommission Site o mais cedo possível. O procedimento de desativação será concluído mais rapidamente e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (selecione **Start Decommission** no passo 5 do assistente).


Requisitos adicionais para uma desativação do local desconetado

Antes que o StorageGRID possa remover um site desconetado, você deve garantir o seguinte:


- Contactou o seu representante da conta NetApp. O NetApp revisará seus requisitos antes de ativar todas as etapas no assistente do site de desintegração.



Você não deve tentar uma desativação de site desconetada se você acredita que pode ser possível recuperar o site ou recuperar quaisquer dados de objeto do site.

- Todos os nós no local devem ter um estado de conexão de um dos seguintes:
 - **Desconhecido** (

566

- Todos os nós em todos os outros locais devem ter um estado de conexão de **conectado** (); no entanto, esses outros nós podem ter alertas ativos.
- Você deve entender que você não poderá mais usar o StorageGRID para visualizar ou recuperar quaisquer dados de objeto que foram armazenados no site. Quando o StorageGRID executa esse procedimento, ele não tenta preservar nenhum dado do local desconetado.



Se suas regras e políticas de ILM foram projetadas para proteger contra a perda de um único site, cópias de seus objetos ainda existem nos sites restantes.

- Você deve entender que se o site continha a única cópia de um objeto, o objeto é perdido e não pode ser recuperado.

Considerações para controles de consistência quando você remove um site

O nível de consistência para um bucket do S3 ou contêiner Swift determina se o StorageGRID replica totalmente os metadados de objetos para todos os nós e sites antes de dizer a um cliente que a ingestão de objetos foi bem-sucedida. Os controles de consistência fornecem um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e locais.

Quando o StorageGRID remove um site, ele precisa garantir que nenhum dado seja gravado no site que está sendo removido. Como resultado, ele substitui temporariamente o nível de consistência para cada bucket ou contentor. Depois de iniciar o processo de desativação do site, o StorageGRID usa temporariamente a consistência forte do site para impedir que os metadados de objetos sejam gravados no site sejam removidos.

Como resultado dessa substituição temporária, esteja ciente de que qualquer operação de gravação, atualização e exclusão do cliente que ocorrer durante a desativação de um site pode falhar se vários nós ficarem indisponíveis nos locais restantes.

Informações relacionadas

[Como a recuperação do local é realizada pelo suporte técnico](#)

[Gerenciar objetos com ILM](#)

[Expanda sua grade](#)

Reúna os materiais necessários

Antes de desativar um site, você deve obter os seguintes materiais.

Item	Notas
Arquivo do pacote de recuperação .zip	Tem de transferir o ficheiro de pacote de recuperação mais recente .zip(sgws-recovery-package-id-revision.zip). Você pode usar o arquivo Pacote de recuperação para restaurar o sistema se ocorrer uma falha.
Passwords.txt ficheiro	Este arquivo contém as senhas necessárias para acessar os nós de grade na linha de comando e está incluído no Pacote de recuperação.

Frase-passe do provisionamento	A frase-passe é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no <code>Passwords.txt</code> arquivo.
Descrição da topologia do sistema StorageGRID antes da desativação	Se disponível, obtenha qualquer documentação que descreva a topologia atual do sistema.

Informações relacionadas

[Requisitos do navegador da Web](#)

[Faça o download do pacote de recuperação](#)

Passo 1: Selecione Site

Para determinar se um site pode ser desativado, comece acessando o assistente Decommission Site.

O que você vai precisar

- Você deve ter obtido todos os materiais necessários.
- Você deve ter revisado as considerações para remover um site.
- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter a permissão de acesso root ou as permissões Manutenção e ILM.

Passos

1. Selecione **MAINTENANCE > Tasks > Decommission**.
2. Selecione **Decommission Site**.

O passo 1 (Selecionar local) do assistente Decommission Site aparece. Esta etapa inclui uma lista alfabética dos sites no seu sistema StorageGRID.

Decommission Site

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

Site Name	Used Storage Capacity	Decommission Possible
<input type="radio"/> Raleigh	3.93 MB	
<input type="radio"/> Sunnyvale	3.97 MB	
<input type="radio"/> Vancouver	3.90 MB	No. This site contains the primary Admin Node.

[Next](#)

3. Visualize os valores na coluna **capacidade de armazenamento usada** para determinar quanto armazenamento está sendo usado atualmente para dados de objeto em cada local.

A capacidade de armazenamento utilizada é uma estimativa. Se os nós estiverem offline, a capacidade de armazenamento usada será o último valor conhecido para o site.

- Para uma desativação de um site conectado, esse valor representa a quantidade de dados de objetos que precisarão ser movidos para outros sites ou excluídos pelo ILM antes de poder desativar este site com segurança.
- Para uma desativação de um site desconectado, esse valor representa quanto do armazenamento de dados do seu sistema ficará inacessível quando você desativar este site.



Se sua política de ILM foi projetada para proteger contra a perda de um único site, cópias de seus dados de objeto ainda devem existir nos sites restantes.

4. Reveja as razões na coluna **Decommission possible** para determinar quais sites podem ser desativados atualmente.



Se houver mais de um motivo pelo qual um site não pode ser desativado, o motivo mais crítico é mostrado.

Desativar possível motivo	Descrição	Próximo passo
Marca de verificação verde ()	Você pode desativar este site.	Vá para o próximo passo .

Desativar possível motivo	Descrição	Próximo passo
Não. Este site contém o nó de administração principal.	Não é possível desativar um site que contém o nó de administração principal.	Nenhum. Não é possível executar este procedimento.
Não. Este site contém um ou mais nós de arquivo.	Não é possível desativar um site que contém um nó de arquivo.	Nenhum. Não é possível executar este procedimento.
Não. Todos os nós neste local estão desconetados. Contacte o representante da sua conta NetApp.	Não é possível executar uma desativação do site conetado a menos que cada nó no site esteja conetado (✔).	Se você quiser executar uma desativação do site desconetada, entre em Contato com seu representante da conta do NetApp, que revisará seus requisitos e ativará o restante do assistente do site de desintegração. IMPORTANTE: Nunca coloque os nós online offline para que você possa remover um site. Você perderá dados.

O exemplo mostra um sistema StorageGRID com três locais. A marca de seleção verde (✔) para os sites Raleigh e Sunnyvale indica que você pode desativar esses sites. No entanto, você não pode desativar o site Vancouver porque ele contém o nó Admin principal.

1. Se for possível desativar, selecione o botão de opção do site.

O botão **Next** está ativado.

2. Selecione **seguinte**.

A etapa 2 (Exibir detalhes) é exibida.

Passo 2: Ver detalhes

Na Etapa 2 (Exibir detalhes) do assistente Decommission Site, você pode analisar quais nós estão incluídos no site, ver quanto espaço foi usado em cada nó de armazenamento e avaliar quanto espaço livre está disponível nos outros sites da sua grade.

O que você vai precisar

Antes de desativar um site, você deve rever a quantidade de dados de objeto existentes no site.

- Se você estiver executando uma desativação de um site conetado, você deve entender a quantidade de dados de objeto atualmente existentes no site antes de atualizar o ILM. Com base nas capacidades do site e nas necessidades de proteção de dados, você pode criar novas regras de ILM para mover dados para outros sites ou excluir dados de objeto do site.
- Execute as expansões necessárias do nó de armazenamento antes de iniciar o procedimento de desativação, se possível.
- Se você estiver executando uma desativação de site desconetada, você deve entender a quantidade de

dados de objeto ficarão permanentemente inacessíveis quando você remover o site.

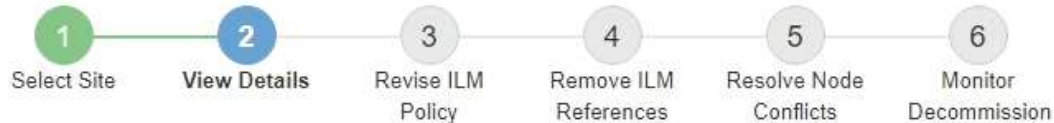


Se você estiver executando uma desativação de site desconetada, o ILM não poderá mover ou excluir dados de objeto. Quaisquer dados que permaneçam no site serão perdidos. No entanto, se sua política de ILM foi projetada para proteger contra a perda de um único site, cópias de seus dados de objeto ainda existem nos sites restantes.

Passos

1. No passo 2 (Ver detalhes), reveja quaisquer avisos relacionados com o site que selecionou para remover.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

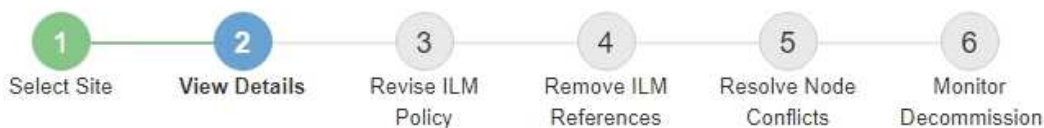
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

Nestes casos, aparece um aviso:

- O site inclui um Gateway Node. Se os clientes S3 e Swift estiverem se conectando atualmente a esse nó, você deverá configurar um nó equivalente em outro site. Certifique-se de que os clientes podem se conectar ao nó de substituição antes de continuar com o procedimento de desativação.
- O local contém uma mistura de nós conectados (✅) e desconectados (🌙 ou 🔄). Antes de remover este site, você deve colocar todos os nós offline de volta online.

2. Reveja os detalhes sobre o site que selecionou para remover.

Decommission Site



Raleigh Details

Number of Nodes: 3 Free Space: 475.38 GB
Used Space: 3.93 MB Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Previous

Next

As seguintes informações estão incluídas para o site selecionado:

- Número de nós
- O espaço total usado, o espaço livre e a capacidade de todos os nós de storage no local.
 - Para uma desativação de um site conectado, o valor **espaço usado** representa a quantidade de dados de objeto que devem ser movidos para outros sites ou excluídos com o ILM.
 - Para uma desativação do site desconectada, o valor **espaço usado** indica a quantidade de dados de objeto ficarão inacessíveis quando você remover o site.
- Nomes de nós, tipos e estados de conexão:
 - (Ligado)
 - (Administrativamente para baixo)
 - (Desconhecido)
- Detalhes sobre cada nó:
 - Para cada nó de storage, a quantidade de espaço que foi usada para dados de objeto.

- Para nós de administração e nós de gateway, se o nó é usado atualmente em um grupo de alta disponibilidade (HA). Não é possível desativar um nó de administrador ou um nó de gateway usado em um grupo de HA. Antes de iniciar a desativação, é necessário editar grupos de HA para remover todos os nós do local. Você também pode remover o grupo de HA se ele incluir somente nós deste local.

Administrar o StorageGRID

3. Na seção Detalhes para outros sites da página, avalie quanto espaço está disponível nos outros sites da sua grade.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB

Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Se você estiver executando uma desativação do site conectado e planeja usar o ILM para mover dados de objetos do site selecionado (em vez de apenas excluí-lo), você deve garantir que os outros sites tenham capacidade suficiente para acomodar os dados movidos e que a capacidade adequada permaneça para crescimento futuro.



Um aviso aparece se o **espaço usado** para o site que você deseja remover for maior que o **espaço livre total para outros sites**. Para garantir que a capacidade de armazenamento adequada esteja disponível após a remoção do local, talvez seja necessário executar uma expansão antes de executar este procedimento.

4. Selecione **seguinte**.

O passo 3 (revisar política ILM) é exibido.

Informações relacionadas

[Gerenciar objetos com ILM](#)

Passo 3: Revise a Política de ILM

A partir do passo 3 (rever a política ILM) do assistente do site de desintegração, você pode determinar se o site é referido pela política ILM ativa.

O que você vai precisar

Você tem uma boa compreensão de como o ILM funciona e está familiarizado com a criação de pools de armazenamento, perfis de codificação de apagamento, regras ILM e simulação e ativação de uma política ILM.

[Gerenciar objetos com ILM](#)

Sobre esta tarefa

O StorageGRID não pode desativar um site se esse site for referido por qualquer regra ILM na política ILM ativa.

Se sua política ILM atual se refere ao site que você deseja remover, você deve ativar uma nova política ILM que atenda a certos requisitos. Especificamente, a nova política ILM:

- Não é possível usar um pool de armazenamento que se refere ao site.
- Não é possível usar um perfil de codificação de apagamento que se refere ao site.
- Não é possível usar o pool de armazenamento padrão **todos os nós de armazenamento** ou o site padrão **todos os sites**.
- Não é possível usar a regra de estoque **Make 2 copies**.
- Deve ser projetado para proteger totalmente todos os dados de objetos.



Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. Uma regra de ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Se você estiver executando um *Connected site Dedescomissionar*, você deve considerar como o StorageGRID deve gerenciar os dados do objeto atualmente no site que você deseja remover. Dependendo dos requisitos de proteção de dados, as novas regras podem mover os dados de objetos existentes para diferentes locais ou excluir quaisquer cópias de objetos extras que não sejam mais necessárias.

Entre em Contato com o suporte técnico se precisar de assistência para projetar a nova política.

Passos

1. Na Etapa 3 (revisar a Política ILM), determine se alguma regra ILM na política ILM ativa se refere ao site que você selecionou para remover.

Decommission Site



If your current ILM policy refers to the site, you must activate a new policy before you can go to the next step.

The new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the **Make 2 Copies** rule.
- Must be designed to fully protect all object data after one site is removed.

Contact technical support if you need assistance in designing the new policy.

If you are performing a connected site decommission, StorageGRID will begin to remove object data from the site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks, but you can safely start a site decommission while object data still exists at the site.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: [Data Protection for Three Sites](#)

The active ILM policy refers to Raleigh. Before you can remove this site, you must propose and activate a new policy.

Name	EC Profiles	Storage Pools
3 copies for S3 tenant	—	Raleigh storage pool
2 copy 2 sites for smaller objects	—	Raleigh storage pool
EC for larger objects	three site EC profile	All 3 Sites

Previous

Next

2. Se nenhuma regra estiver listada, selecione **Next** para ir para a Etapa 4 (Remover referências ILM)

Passo 4: Remover referências ILM

3. Se uma ou mais regras ILM estiverem listadas na tabela, selecione o link ao lado de **Nome da política ativa**.

A página de políticas ILM aparece em uma nova guia do navegador. Use esta guia para atualizar o ILM. A página Decommission Site permanecerá aberta na outra guia.

- a. Se necessário, selecione **ILM Storage Pools** para criar um ou mais pools de armazenamento que não se referem ao site.



Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

- b. Se você planeja usar a codificação de apagamento, selecione **ILM codificação de apagamento** para criar um ou mais perfis de codificação de apagamento.

Você deve selecionar pools de armazenamento que não se referem ao site.



Não use o pool de storage **todos os nós de storage** nos perfis de codificação de apagamento.

4. Selecione **ILM Rules** e clone cada uma das regras listadas na tabela para a Etapa 3 (revisar a Política ILM).



Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

- a. Use nomes que facilitem a seleção dessas regras em uma nova política.
- b. Atualize as instruções de colocação.

Remova todos os pools de storage ou perfis de codificação de apagamento que se referem ao site e substitua-os por novos pools de armazenamento ou perfis de codificação de apagamento.



Não use o pool de armazenamento **todos os nós de storage** nas novas regras.

5. Selecione **ILM Policies** e crie uma nova política que use as novas regras.



Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

- a. Selecione a política ativa e selecione **Clone**.
- b. Especifique um nome de política e um motivo para a alteração.
- c. Selecione regras para a política clonada.
 - Desmarque todas as regras listadas para a Etapa 3 (revisar a Política ILM) da página do site de desintegração.
 - Selecione uma regra padrão que não se refira ao site.



Não selecione a regra **Make 2 Copies** porque essa regra usa o pool de armazenamento **All Storage Nodes**, que não é permitido.

- Selecione as outras regras de substituição que criou. Essas regras não devem se referir ao site.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

	Rule Name
<input checked="" type="radio"/>	2 copies at Sunnyvale and Vancouver for smaller objects
<input type="radio"/>	2 copy 2 sites for smaller objects
<input type="radio"/>	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

	Rule Name	Tenant Account
<input type="checkbox"/>	3 copies for S3 tenant	S3 (61659555232085399385)
<input type="checkbox"/>	EC for larger objects	—
<input checked="" type="checkbox"/>	1-site EC for larger objects	—
<input checked="" type="checkbox"/>	2 copies for S3 tenant	S3 (61659555232085399385)

Cancel

Apply

d. Selecione **aplicar**.

e. Arraste e solte as linhas para reordenar as regras na política.

Não é possível mover a regra padrão.



Você deve confirmar se as regras ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando na parte superior.

a. Salve a política proposta.

6. Ingrida objetos de teste e simule a política proposta para garantir que as regras corretas sejam aplicadas.



Erros em uma política ILM podem causar perda de dados irrecoverável. Analise e simule cuidadosamente a política antes de ativá-la para confirmar que funcionará como pretendido.



Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise todas as alterações no posicionamento de objetos replicados e codificados por apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas de recursos temporários quando os novos posicionamentos são avaliados e implementados.

7. Ative a nova política.

Se você estiver executando uma desativação do site conetado, o StorageGRID começará a remover os dados do objeto do site selecionado assim que você ativar a nova política ILM. Mover ou excluir todas as cópias de objetos pode levar semanas. Embora você possa iniciar com segurança uma desativação do site enquanto os dados do objeto ainda existirem no site, o procedimento de desativação será concluído

com mais rapidez e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (selecionando **Start Decommission** no passo 5 do assistente).

- Volte para **passo 3 (revisar a política ILM)** para garantir que nenhuma regra ILM na nova política ativa consulte o site e o botão **Next** esteja ativado.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: [Data Protection for Two Sites](#) 

No ILM rules in the active ILM policy refer to Raleigh.

Previous

Next



Se alguma regra estiver listada, você deve criar e ativar uma nova política ILM antes de continuar.

- Se nenhuma regra estiver listada, selecione **Next**.

O passo 4 (Remover referências ILM) é exibido.

Passo 4: Remover referências ILM

No passo 4 (Remover referências ILM) do assistente Decommission Site, você pode remover a política proposta se existir e excluir ou editar quaisquer regras ILM não utilizadas que ainda se referem ao site.

Sobre esta tarefa

Você está impedido de iniciar o procedimento de desativação do site nestes casos:

- Existe uma política proposta de ILM. Se você tem uma política proposta, você deve excluí-la.
- Qualquer regra ILM refere-se ao site, mesmo que essa regra não seja usada em nenhuma política ILM. Você deve excluir ou editar todas as regras que se referem ao site.

Passos

- Se uma política proposta for listada, remova-a.


Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

Proposed policy exists ▲

You must delete the proposed policy before you can start the site decommission procedure.

Policy name: [Data Protection for Two Sites \(v2\)](#)  [Delete Proposed Policy](#)

4 ILM rules refer to Raleigh ▼

1 Erasure Coding profile will be deactivated ▼

3 storage pools will be deleted ▼

[Previous](#) [Next](#)

- a. Selecione **Excluir Política proposta**.
 - b. Selecione **OK** na caixa de diálogo de confirmação.
2. Determine se quaisquer regras de ILM não utilizadas se referem ao site.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

4 ILM rules refer to Data Center 3 ▲

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

[Go to the ILM Rules page](#)

Name	EC Profiles	Storage Pools	Delete
Make 2 Copies	—	All Storage Nodes	
3 copies for S3 tenant	—	Raleigh storage pool	
2 copies 2 sites for smaller objects	—	Raleigh storage pool	
EC larger objects	three site EC profile	All 3 Sites	

1 Erasure Coding profile will be deactivated ▼

3 storage pools will be deleted ▼

Todas as regras ILM que estão listadas ainda se referem ao site, mas não são usadas em nenhuma política. No exemplo:

- A regra de estoque **Make 2 Copies** usa o conjunto de armazenamento padrão do sistema **All Storage Nodes**, que usa o site All Sites.
- A regra não utilizada **3 cópias para S3 inquilino** refere-se ao pool de armazenamento **Raleigh**.
- A regra não utilizada **2 copy 2 sites para objetos menores** refere-se ao pool de armazenamento **Raleigh**.
- As regras não utilizadas para **EC Large Objects** usam o site Raleigh no perfil de codificação de apagamento **All 3 Sites**.
- Se nenhuma regra ILM estiver listada, selecione **Next** para ir para **Etapa 5 (resolver conflitos de nó)**.

Etapa 5: Resolver conflitos de nó (e iniciar a desativação)



Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa o site todos os sites.


- Se uma ou mais regras ILM estiverem listadas, vá para a próxima etapa.

3. Edite ou exclua cada regra não utilizada:

- Para editar uma regra, acesse a página regras do ILM e atualize todos os canais que usam um perfil de codificação de apagamento ou um pool de armazenamento que se refere ao site. Em seguida, retorne a **Etapa 4 (Remover referências ILM)**.



Para obter detalhes, consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

- Para excluir uma regra, selecione o ícone de lixeira  e selecione **OK**.



Você deve excluir a regra de estoque **Make 2 Copies** antes de poder desativar um site.

4. Confirme se não existe nenhuma política de ILM proposta, nenhuma regra de ILM não utilizada se refere ao site e o botão **Next** está ativado.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

No ILM rules refer to Raleigh

1 Erasure Coding profile will be deactivated

3 storage pools will be deleted

Previous

Next

5. Selecione **seguinte**.



Quaisquer pools de armazenamento restantes e perfis de codificação de apagamento que se refiram ao site tornar-se-ão inválidos quando o site for removido. Quando o StorageGRID descompacta o site, ele desativará automaticamente quaisquer perfis de codificação de apagamento não utilizados que se refiram ao site e excluirá automaticamente quaisquer pools de armazenamento não utilizados que se refiram ao site. O pool de storage de todos os nós de storage padrão do sistema é removido porque ele usa o site todos os sites.

A etapa 5 (resolver conflitos de nó) é exibida.

Etapa 5: Resolver conflitos de nó (e iniciar a desativação)

Na Etapa 5 (resolver conflitos de nós) do assistente do local de desativação, você pode determinar se algum nó no sistema StorageGRID está desconectado ou se algum nó no local selecionado pertence a um grupo de alta disponibilidade (HA). Depois que qualquer conflito de nó for resolvido, você inicia o procedimento de desativação nesta página.

Você deve garantir que todos os nós do sistema StorageGRID estejam no estado correto, como a seguir:

- Todos os nós do sistema StorageGRID devem estar conectados ().



Se você estiver executando uma desativação do local desconectado, todos os nós do local que você está removendo devem ser desconectados e todos os nós de todos os outros locais devem estar conectados.

- Nenhum nó no local que você está removendo pode ter uma interface que pertence a um grupo de alta disponibilidade (HA).

Se algum nó estiver listado para a Etapa 5 (resolver conflitos de nó), você deve corrigir o problema antes de iniciar a desativação.

Antes de iniciar o procedimento de desativação do site a partir desta página, reveja as seguintes considerações:

- Você deve permitir tempo adequado para que o procedimento de desativação seja concluído.



A migração ou exclusão de dados de objetos de um local pode levar dias, semanas ou até meses, dependendo da quantidade de dados no local, da carga no sistema, das latências de rede e da natureza das mudanças necessárias no ILM.



- Enquanto o procedimento de desativação do site está em execução:
 - Você não pode criar regras ILM que se referem ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para se referir ao site.
 - Não é possível executar outros procedimentos de manutenção, como expansão ou atualização.



Se você precisar executar outro procedimento de manutenção durante a desativação de um site conectado, poderá pausar o procedimento enquanto os nós de storage estiverem sendo removidos. O botão **Pausa** é ativado durante o estágio ""Descomissionamento replicado e eliminação de dados codificados"".

- Se você precisar recuperar qualquer nó depois de iniciar o procedimento de desativação do site, entre em Contato com o suporte.

Passos

1. Consulte a seção nós desconectados da Etapa 5 (resolver conflitos de nó) para determinar se algum nó no sistema StorageGRID tem um estado de conexão desconhecido () ou administrativamente inativo ().

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193	Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase

Previous

Start Decommission

2. Se algum nó estiver desconetado, coloque-o novamente on-line.

Consulte as instruções para monitoramento e solução de problemas do StorageGRID e os procedimentos do nó de grade. Entre em Contato com o suporte técnico se precisar de assistência.

3. Quando todos os nós desconetados forem colocados novamente on-line, consulte a seção grupos de HA da Etapa 5 (resolver conflitos de nó).

Esta tabela lista todos os nós do local selecionado que pertencem a um grupo de alta disponibilidade (HA).

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue:

All grid nodes are connected

1 node in the selected site belongs to an HA group ^

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase ?

Previous

Start Decommission

4. Se algum dos nós estiver listado, faça um dos seguintes procedimentos:

- Edite cada grupo de HA afetado para remover a interface do nó.
- Remover um grupo de HA que inclua somente nós deste local. Consulte as instruções para administrar o StorageGRID.

Se todos os nós estiverem conectados e nenhum nó no local selecionado for usado em um grupo de HA, o campo **frase-passe de provisionamento** será ativado.

5. Introduza a frase-passe de provisionamento.

O botão **Start Decommission** fica ativado.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase 

Previous

Start Decommission

6. Se você estiver pronto para iniciar o procedimento de desativação do site, selecione **Start Decommission**.

Um aviso lista o local e os nós que serão removidos. Você é lembrado que pode levar dias, semanas ou até meses para remover completamente o site.

Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Reveja o aviso. Se estiver pronto para começar, selecione **OK**.

Uma mensagem aparece quando a nova configuração de grade é gerada. Esse processo pode levar algum tempo, dependendo do tipo e do número de nós de grade desativados.

Passphrase

Provisioning Passphrase 

 Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission 

Quando a nova configuração da grade for gerada, o passo 6 (Monitor Decommission) será exibido.



O botão **anterior** permanece desativado até que a desativação esteja concluída.

Informações relacionadas

[Monitorar e solucionar problemas](#)

[Procedimentos do nó de grade](#)

[Administrar o StorageGRID](#)

Passo 6: Monitorar a desintegração

A partir do passo 6 (Monitor Decommission) do assistente de página do site Decommission, você pode monitorar o progresso à medida que o site é removido.

Sobre esta tarefa

Quando o StorageGRID remove um site conectado, ele remove nós nessa ordem:

1. Nós de gateway
2. Nós de administração
3. Nós de storage

Quando o StorageGRID remove um site desconectado, ele remove nós nessa ordem:

1. Nós de gateway
2. Nós de storage
3. Nós de administração

Cada nó de gateway ou nó de administrador pode exigir apenas alguns minutos ou uma hora para ser removido; no entanto, os nós de storage podem levar dias ou semanas.

Passos

1. Assim que um novo pacote de recuperação for gerado, baixe o arquivo.

Decommission Site



i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Baixe o pacote de recuperação o mais rápido possível para garantir que você possa recuperar sua grade se algo der errado durante o procedimento de desativação.

- a. Selecione o link na mensagem ou selecione **MANUTENÇÃO sistema Pacote de recuperação**.
- b. Transfira o .zip arquivo.

Consulte as instruções para [Transferir o pacote de recuperação](#).



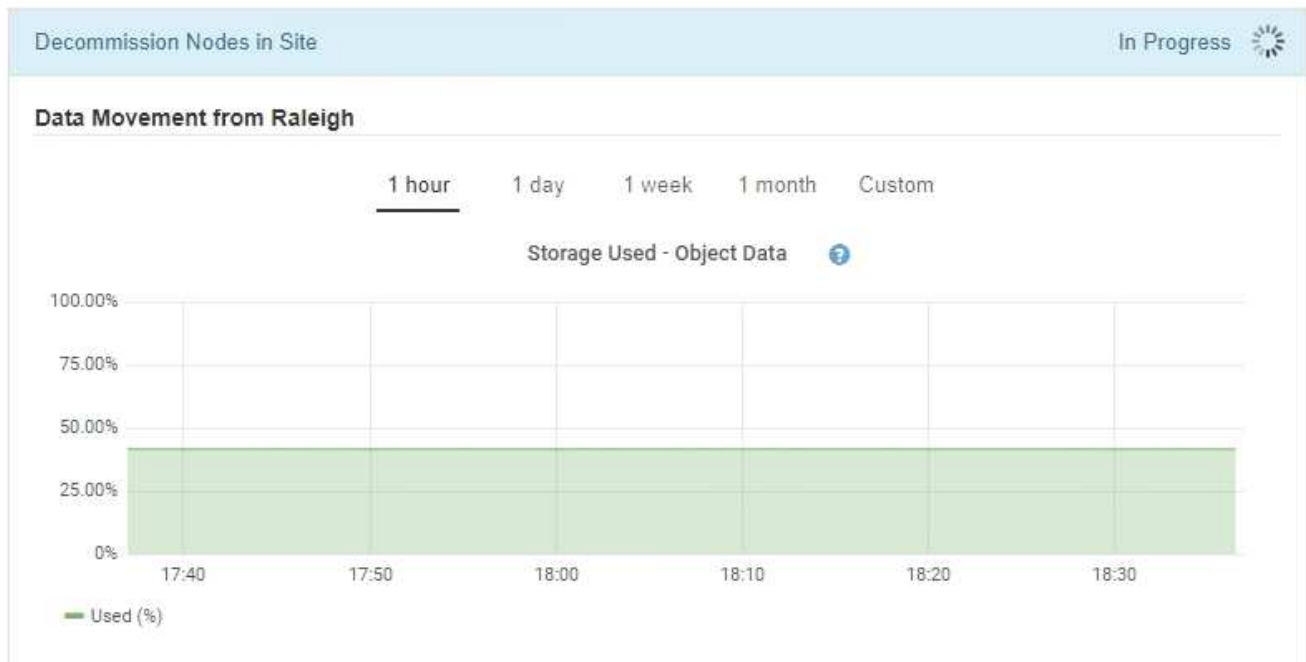
O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

2. Usando o gráfico de movimentação de dados, monitore a movimentação de dados de objetos deste site para outros sites.

A movimentação de dados começou quando você ativou a nova política de ILM no passo 3 (revisar

política de ILM). A movimentação de dados ocorrerá durante todo o procedimento de desativação.

Decommission Site Progress



3. Na seção progresso do nó da página, monitore o andamento do procedimento de desativação à medida que os nós são removidos.

Quando um nó de armazenamento é removido, cada nó passa por uma série de estágios. Embora a maioria desses estágios ocorra rapidamente ou até mesmo imperceptivelmente, talvez seja necessário esperar dias ou até semanas para que outros estágios sejam concluídos, com base na quantidade de dados que precisam ser movidos. É necessário tempo adicional para gerenciar dados codificados de apagamento e reavaliar o ILM.

Node Progress

i Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause
Resume

Name	Type	Progress	Stage
RAL-S1-101-196	Storage Node	<div style="width: 20%; height: 10px; background-color: #00a0e3;"></div>	Decommissioning Replicated and Erasure Coded Data
RAL-S2-101-197	Storage Node	<div style="width: 20%; height: 10px; background-color: #00a0e3;"></div>	Decommissioning Replicated and Erasure Coded Data
RAL-S3-101-198	Storage Node	<div style="width: 20%; height: 10px; background-color: #00a0e3;"></div>	Decommissioning Replicated and Erasure Coded Data

Se você estiver monitorando o progresso de uma desativação de um site conectado, consulte esta tabela para entender os estágios de desativação de um nó de armazenamento:

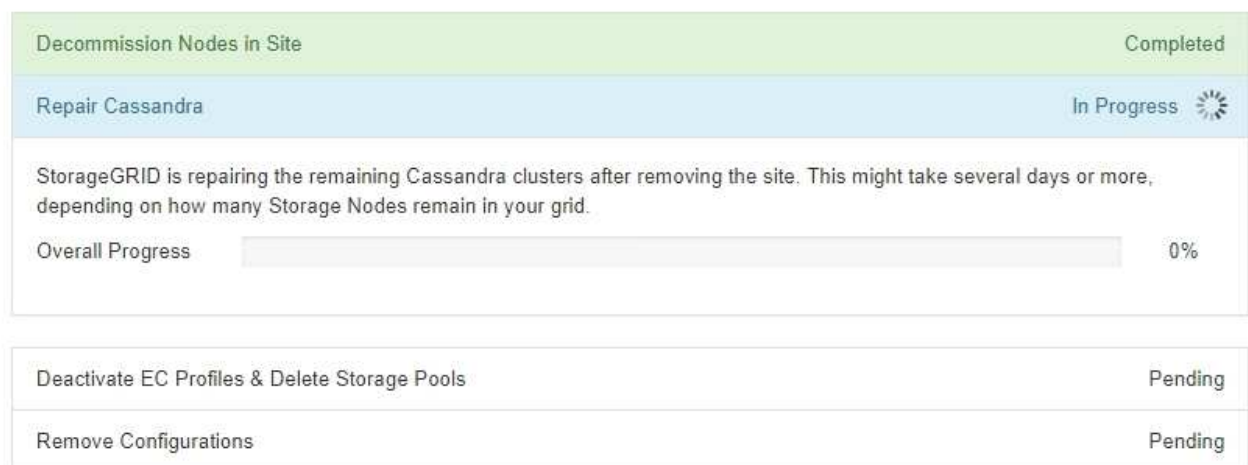
Fase	Duração estimada
Pendente	Minuto ou menos
Aguarde bloqueios	Minutos
Preparar tarefa	Minuto ou menos
Marcação LDR desativada	Minutos
Desativação de dados duplicados e codificados de apagamento	Horas, dias ou semanas com base na quantidade de dados Nota: Se você precisar executar outras atividades de manutenção, você pode pausar a desativação do site durante essa etapa.
Estado definido LDR	Minutos
Lavar filas Auditoria	Minutos a horas, com base no número de mensagens e na latência da rede.
Concluído	Minutos

Se você estiver monitorando o andamento de uma desativação de um local desconectado, consulte esta tabela para entender os estágios de desativação de um nó de armazenamento:

Fase	Duração estimada
Pendente	Minuto ou menos
Aguarde bloqueios	Minutos
Preparar tarefa	Minuto ou menos
Desativar Serviços Externos	Minutos
Revogação do certificado	Minutos
Anular registo nó	Minutos
Anular registo de grau de armazenamento	Minutos
Remoção do Grupo de armazenamento	Minutos
Remoção da entidade	Minutos
Concluído	Minutos

4. Depois de todos os nós terem atingido a etapa completa, aguarde que as restantes operações de desativação do local sejam concluídas.
- Durante a etapa **reparar Cassandra**, o StorageGRID faz todos os reparos necessários aos clusters do Cassandra que permanecem em sua grade. Esses reparos podem levar vários dias ou mais, dependendo de quantos nós de storage permanecem na grade.

Decommission Site Progress



- Durante a etapa **Deactivate EC Profiles Delete Storage Pools**, as seguintes alterações de ILM são feitas:
 - Todos os perfis de codificação de apagamento que se referem ao site são desativados.
 - Todos os pools de armazenamento que se referem ao site são excluídos.



O pool de storage de todos os nós de storage padrão do sistema também é removido porque ele usa o site todos os sites.

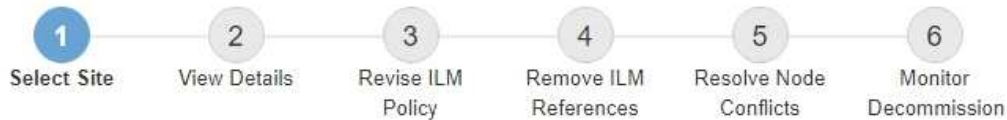
- Finalmente, durante a etapa **Remove Configuration**, quaisquer referências restantes ao site e seus nós são removidas do resto da grade.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Quando o procedimento de desativação for concluído, a página Decommission Site (local de desativação) mostra uma mensagem de sucesso e o local removido não é mais apresentado.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity	Decommission Possible
<input checked="" type="radio"/>	Sunnyvale	4.79 MB	
<input type="radio"/>	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Depois de terminar

Conclua estas tarefas após concluir o procedimento de desativação do local:

- Certifique-se de que as unidades de todos os nós de storage no local desativado sejam limpas. Utilize uma ferramenta ou serviço de limpeza de dados disponíveis no mercado para remover dados das

unidades de forma permanente e segura.

- Se o site incluiu um ou mais nós de administração e logon único (SSO) estiver ativado para o seu sistema StorageGRID, remova todas as confianças de parte que dependem do site dos Serviços de Federação do ativo Directory (AD FS).
- Depois que os nós tiverem sido desligados automaticamente como parte do procedimento de desativação do site conectado, remova as máquinas virtuais associadas.

Procedimentos de manutenção da rede

Atualizar sub-redes para rede de Grade

O StorageGRID mantém uma lista das sub-redes de rede usadas para se comunicar entre nós de grade na rede de grade (eth0). Essas entradas incluem as sub-redes usadas para a rede de Grade por cada site em seu sistema StorageGRID, bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados através do gateway rede de Grade. Quando você adiciona nós de grade ou um novo site em uma expansão, talvez seja necessário atualizar ou adicionar sub-redes à rede de Grade.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter os endereços de rede, na notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se você estiver executando uma atividade de expansão que inclua a adição de uma nova sub-rede, será necessário adicionar a nova sub-rede da grade antes de iniciar o procedimento de expansão.

Passos

1. Selecione **MAINTENANCE > Network > Grid Network**.

Grid Network

Configure the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network (eth0) for each site in your StorageGRID system as well as any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnets

Subnet 1



Passphrase

Provisioning
Passphrase

Save

2. Na lista de sub-redes, clique no sinal de mais para adicionar uma nova sub-rede na notação CIDR.

Por exemplo, introduza 10.96.104.0/22.

3. Digite a senha de provisionamento e clique em **Salvar**.

As sub-redes especificadas são configuradas automaticamente para o sistema StorageGRID.

4. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.

a. Selecione **MAINTENANCE > System > Recovery package**.

b. Introduza a frase-passe de provisionamento.

Configurar endereços IP

Você pode executar a configuração de rede configurando endereços IP para nós de grade usando a ferramenta alterar IP.

Você deve usar a ferramenta alterar IP para fazer a maioria das alterações na configuração de rede que foi inicialmente definida durante a implantação de grade. As alterações manuais usando comandos e arquivos de rede padrão do Linux podem não se propagar para todos os serviços do StorageGRID e podem não persistir em atualizações, reinicializações ou procedimentos de recuperação de nós.



Se pretender alterar o endereço IP da rede de grade para todos os nós da grade, utilize o [procedimento especial para mudanças em toda a grade](#).



Se você estiver fazendo alterações somente na Lista de sub-redes de rede de Grade, use o Gerenciador de Grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta alterar IP se o Gerenciador de Grade estiver inacessível devido a um problema de configuração de rede, ou você estiver executando uma alteração de roteamento de rede de Grade e outras alterações de rede ao mesmo tempo.



O procedimento de mudança de IP pode ser um procedimento disruptivo. Partes da grade podem estar indisponíveis até que a nova configuração seja aplicada.

- Interfaces Ethernet*

O endereço IP atribuído a eth0 é sempre o endereço IP da rede de Grade do nó da grade. O endereço IP atribuído ao eth1 é sempre o endereço IP da rede Admin do nó da grade. O endereço IP atribuído ao eth2 é sempre o endereço IP da rede do cliente do nó da grade.

Observe que em algumas plataformas, como dispositivos StorageGRID, eth0, eth1 e eth2, podem ser interfaces agregadas compostas por bridges subordinadas ou ligações de interfaces físicas ou VLAN. Nessas plataformas, a guia **SSM > recursos** pode mostrar o endereço IP de rede, administrador e rede cliente atribuído a outras interfaces além de eth0, eth1 ou eth2.

DHCP

Só pode configurar o DHCP durante a fase de implementação. Não é possível configurar o DHCP durante a configuração. Você deve usar os procedimentos de alteração de endereço IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. O uso da ferramenta Change IP fará com que os endereços DHCP fiquem estáticos.

Grupos de alta disponibilidade (HA)

- Se uma interface de rede do cliente estiver contida em um grupo HA, não será possível alterar o endereço IP da rede do cliente dessa interface para um endereço que esteja fora da sub-rede configurada para o grupo HA.
- Não é possível alterar o endereço IP da rede do cliente para o valor de um endereço IP virtual existente atribuído a um grupo HA configurado na interface rede do cliente.
- Se uma interface de rede Grid estiver contida em um grupo HA, você não poderá alterar o endereço IP da rede Grid dessa interface para um endereço fora da sub-rede configurada para o grupo HA.
- Não é possível alterar o endereço IP da rede de Grade para o valor de um endereço IP virtual existente atribuído a um grupo HA configurado na interface rede de Grade.

Alterar a configuração da rede do nó

Você pode alterar a configuração de rede de um ou mais nós usando a ferramenta alterar IP. Você pode alterar a configuração da rede de Grade ou adicionar, alterar ou remover as redes Admin ou Client.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

- Linux:* se você estiver adicionando um nó de grade à rede Admin ou rede de cliente pela primeira vez, e você não tiver configurado anteriormente `ADMIN_network_TARGET` ou `CLIENT_network_TARGET` no arquivo de configuração do nó, você deve fazê-lo agora.

Consulte as instruções de instalação do StorageGRID para seu sistema operacional Linux.

Appliances: em appliances StorageGRID, se o cliente ou a rede de administração não tiver sido configurada no Instalador de appliance StorageGRID durante a instalação inicial, a rede não poderá ser adicionada usando apenas a ferramenta Change IP (alterar IP). Primeiro, você deve [coloque o aparelho no modo de manutenção](#) configurar os links, retornar o dispositivo ao modo de operação normal e usar a ferramenta alterar IP para modificar a configuração de rede. Consulte o procedimento para configurar links de rede nas instruções de instalação e manutenção do seu aparelho.

Você pode alterar o endereço IP, a máscara de sub-rede, o gateway ou o valor MTU para um ou mais nós em qualquer rede.

Você também pode adicionar ou remover um nó de uma rede de cliente ou de uma rede de administração:

- Você pode adicionar um nó a uma rede cliente ou a uma rede Admin adicionando um endereço IP/máscara de sub-rede nessa rede ao nó.
- Você pode remover um nó de uma rede de cliente ou de uma rede de administrador excluindo o endereço IP/máscara de sub-rede do nó nessa rede.

Os nós não podem ser removidos da rede de Grade.



Swaps de endereço IP não são permitidos. Se for necessário trocar endereços IP entre nós de grade, você deverá usar um endereço IP intermediário temporário.



Se o logon único (SSO) estiver ativado para o sistema StorageGRID e você estiver alterando o endereço IP de um nó Admin, esteja ciente de que qualquer confiança de parte confiável que foi configurada usando o endereço IP do nó Admin (em vez de seu nome de domínio totalmente qualificado, conforme recomendado) se tornará inválida. Você não poderá mais entrar no nó. Imediatamente após alterar o endereço IP, você deve atualizar ou reconfigurar a confiança de parte confiável do nó nos Serviços de Federação do ative Directory (AD FS) com o novo endereço IP. Consulte as instruções para administrar o StorageGRID.



Todas as alterações feitas na rede usando a ferramenta Change IP são propagadas para o firmware do instalador dos dispositivos StorageGRID. Dessa forma, se o software StorageGRID for reinstalado em um dispositivo ou se um dispositivo for colocado no modo de manutenção, a configuração de rede estará correta.

Passos

1. Faça login no nó de administração principal:

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

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

2. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`

3. Insira a senha de provisionamento no prompt.

É apresentado o menu principal.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. Opcionalmente, selecione 1 para escolher quais nós atualizar. Em seguida, selecione uma das seguintes opções:

- 1: Nó único — selecione pelo nome
- 2: Nó único — selecione por site e, em seguida, por nome
- 3: Nó único — selecione por IP atual
- 4: Todos os nós em um local

- **5:** Todos os nós na grade

Observação: se você quiser atualizar todos os nós, permita que "todos" permaneçam selecionados.

Depois de fazer sua seleção, o menu principal é exibido, com o campo **Selected Nodes** atualizado para refletir sua escolha. Todas as ações subsequentes são realizadas apenas nos nós exibidos.

5. No menu principal, selecione a opção **2** para editar informações de IP/máscara, gateway e MTU para os nós selecionados.

a. Selecione a rede onde deseja fazer alterações:

- **1:** Rede de rede
- **2:** Rede de administração
- **3:** Rede de clientes
- **4:** Todas as redes depois de selecionar, o prompt mostra o nome do nó, o nome da rede (Grade, Admin ou Cliente), o tipo de dados (IP/máscara, Gateway ou MTU) e o valor atual.

Editar o endereço IP, o comprimento do prefixo, o gateway ou MTU de uma interface configurada por DHCP alterará a interface para estática. Quando você seleciona alterar uma interface configurada pelo DHCP, um aviso é exibido para informá-lo de que a interface mudará para estática.

As interfaces configuradas como *fixed* não podem ser editadas.

b. Para definir um novo valor, introduza-o no formato apresentado para o valor atual.

c. Para deixar o valor atual inalterado, pressione **Enter**.

d. Se o tipo de dados for `IP/mask`, você poderá excluir o Admin ou a rede do cliente do nó inserindo **d** ou **0,0.0,0/0**.

e. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

Suas alterações são mantidas até serem limpas ou aplicadas.

6. Reveja as alterações selecionando uma das seguintes opções:

- **5:** Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída do exemplo:

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- 6: Mostra edições na saída que exibe a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando a formatação strikethrough. A exibição adequada depende do cliente terminal que suporta as seqüências de escape VT100 necessárias.

7. Selecione a opção 7 para validar todas as alterações.

Essa validação garante que as regras para redes Grid, Admin e Client, como não usar sub-redes sobrepostas, não sejam violadas.

Neste exemplo, a validação retornou erros.

```

Validating new networking configuration... FAILED.

DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

Neste exemplo, a validação passou.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

8. Depois que a validação passar, escolha uma das seguintes opções:

- **8:** Salve as alterações não aplicadas.

Essa opção permite que você saia da ferramenta Change IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

- **10:** Aplicar a nova configuração de rede.

9. Se você selecionou a opção **10**, escolha uma das seguintes opções:

- **Apply:** Aplique as alterações imediatamente e reinicie automaticamente cada nó, se necessário.

Se a nova configuração de rede não exigir alterações físicas de rede, você pode selecionar **Apply** para aplicar as alterações imediatamente. Os nós serão reiniciados automaticamente, se necessário. Os nós que precisam ser reiniciados serão exibidos.

- **Stage:** Aplique as alterações na próxima vez que os nós forem reiniciados manualmente.

Se você precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, use a opção **stage**, encerre os nós afetados, faça as alterações de rede física necessárias e reinicie os nós afetados. Se você selecionar **Apply** sem primeiro fazer essas alterações de rede, as alterações geralmente falharão.



Se você usar a opção **stage**, será necessário reiniciar o nó o mais rápido possível após o preparo para minimizar as interrupções.

- **Cancelar:** Não faça alterações na rede neste momento.

Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o impacto do usuário. Selecionar **CANCEL** retorna ao menu principal e preserva as alterações para que você possa aplicá-las mais tarde.

Quando você seleciona **Apply** ou **stage**, um novo arquivo de configuração de rede é gerado, o provisionamento é executado e os nós são atualizados com novas informações de trabalho.

Durante o provisionamento, a saída exibe o status à medida que as atualizações são aplicadas.

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

Depois de aplicar ou preparar alterações, um novo pacote de recuperação é gerado como resultado da alteração da configuração da grade.

10. Se você selecionou **stage**, siga estas etapas após a conclusão do provisionamento:

a. Faça as alterações de rede física ou virtual necessárias.

- Alterações físicas de rede*: Faça as alterações físicas necessárias de rede, desligando o nó com segurança, se necessário.
- Linux*: Se você estiver adicionando o nó a uma rede Admin ou rede de cliente pela primeira vez,

certifique-se de que você adicionou a interface conforme descrito em ""adicionando interfaces a um nó existente".

b. Reinicie os nós afetados.

11. Selecione **0** para sair da ferramenta Change IP após a conclusão das alterações.

12. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.

a. Selecione **MAINTENANCE > System > Recovery package**.

b. Introduza a frase-passe de provisionamento.

Informações relacionadas

[Linux: Adicione interfaces ao nó existente](#)

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

[Aparelhos de serviços SG100 e SG1000](#)

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[Administrar o StorageGRID](#)

[Configurar endereços IP](#)

Adicionar ou alterar listas de sub-rede na rede Admin

Você pode adicionar, excluir ou alterar as sub-redes na Lista de sub-redes de rede Admin de um ou mais nós.

O que você vai precisar

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

Você pode adicionar, excluir ou alterar sub-redes para todos os nós na Lista de sub-redes de rede Admin.

Passos

1. Faça login no nó de administração principal:

a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`

3. Insira a senha de provisionamento no prompt.

É apresentado o menu principal.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. Opcionalmente, limite as redes/nós nos quais as operações são executadas. Escolha uma das seguintes opções:

- Selecione os nós a editar escolhendo **1**, se você quiser filtrar em nós específicos nos quais executar a operação. Selecione uma das seguintes opções:
 - **1**: Nó único (selecionar pelo nome)
 - **2**: Nó único (selecione por site, depois pelo nome)
 - **3**: Nó único (selecionar por IP atual)
 - **4**: Todos os nós em um local
 - **5**: Todos os nós na grade
 - **0**: Volte
- Permitir que "all" permaneça selecionado. Após a seleção ser feita, é apresentado o ecrã do menu principal. O campo nós selecionados reflete sua nova seleção e agora todas as operações selecionadas serão executadas somente neste item.

5. No menu principal, selecione a opção para editar sub-redes para a rede Admin (opção **3**).

6. Escolha uma das seguintes opções:

- Adicione uma sub-rede inserindo este comando: `add CIDR`
- Exclua uma sub-rede inserindo este comando: `del CIDR`
- Defina a lista de sub-redes inserindo este comando: `set CIDR`



Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Você pode reduzir a quantidade de digitação necessária usando "seta para cima" para recuperar valores digitados anteriormente para o prompt de entrada atual e, em seguida, editá-los, se necessário.

A entrada de exemplo abaixo mostra a adição de sub-redes à Lista de sub-redes de Admin Network:

```

Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
10.0.0.0/8
172.19.0.0/16
172.21.0.0/16
172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16

```

7. Quando estiver pronto, digite **q** para voltar à tela do menu principal. Suas alterações são mantidas até serem limpas ou aplicadas.



Se você selecionou qualquer um dos modos de seleção de nó "todos" na etapa 2, você deve pressionar **Enter** (sem **q**) para chegar ao próximo nó na lista.

8. Escolha uma das seguintes opções:

- Selecione a opção **5** para mostrar as edições na saída que estão isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída de exemplo abaixo:

```

=====
Site: Data Center 1
=====
DC1-ADM1-105-154 Admin Subnets
                                     add 172.17.0.0/16
                                     del 172.16.0.0/16
                                     [ 172.14.0.0/16 ]
                                     [ 172.15.0.0/16 ]
                                     [ 172.17.0.0/16 ]
                                     [ 172.19.0.0/16 ]
                                     [ 172.20.0.0/16 ]
                                     [ 172.21.0.0/16 ]
Press Enter to continue

```

- Selecione a opção **6** para mostrar as edições na saída que exibem a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões). **Nota:** alguns emuladores de terminal podem mostrar adições e exclusões usando a formatação strikethrough.

Quando você tenta alterar a lista de sub-redes, a seguinte mensagem é exibida:

CAUTION: The Admin Network subnet list on the node might contain /32 subnets derived from automatically applied routes that are not persistent. Host routes (/32 subnets) are applied automatically if the IP addresses provided for external services such as NTP or DNS are not reachable using default StorageGRID routing, but are reachable using a different interface and gateway. Making and applying changes to the subnet list will make all automatically applied subnets persistent. If you do not want that to happen, delete the unwanted subnets before applying changes. If you know that all /32 subnets in the list were added intentionally, you can ignore this caution.

Se você não atribuiu especificamente as sub-redes de servidor NTP e DNS a uma rede, o StorageGRID cria uma rota de host (/32) para a conexão automaticamente. Se, por exemplo, você preferir ter uma rota /16 ou /24 para conexão de saída a um servidor DNS ou NTP, você deve excluir a rota /32 criada automaticamente e adicionar as rotas que deseja. Se você não excluir a rota de host criada automaticamente, ela será persistida depois de aplicar quaisquer alterações à lista de sub-redes.



Embora você possa usar essas rotas de host descobertas automaticamente, em geral, você deve configurar manualmente as rotas DNS e NTP para garantir a conectividade.

9. Selecione a opção **7** para validar todas as alterações faseadas.

Essa validação garante que as regras para redes Grid, Admin e Client sejam seguidas, como o uso de sub-redes sobrepostas.

10. Opcionalmente, selecione a opção **8** para guardar todas as alterações faseadas e voltar mais tarde para continuar a efetuar alterações.

Essa opção permite que você saia da ferramenta Change IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

11. Execute um dos seguintes procedimentos:

- Selecione a opção **9** se quiser limpar todas as alterações sem salvar ou aplicar a nova configuração de rede.
- Selecione a opção **10** se estiver pronto para aplicar alterações e provisionar a nova configuração de rede. Durante o provisionamento, a saída exibe o status à medida que as atualizações são aplicadas conforme mostrado na seguinte saída de amostra:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

12. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.

- a. Selecione **MAINTENANCE > System > Recovery package**.
- b. Introduza a frase-passe de provisionamento.

Informações relacionadas

[Configurar endereços IP](#)

Adicionar ou alterar listas de sub-rede na rede de Grade

Você pode usar a ferramenta alterar IP para adicionar ou alterar sub-redes na rede de Grade.

O que você vai precisar

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

Você pode adicionar, excluir ou alterar sub-redes na Lista de sub-redes de rede de Grade. As alterações afetarão o roteamento em todos os nós da grade.



Se você estiver fazendo alterações somente na Lista de sub-redes de rede de Grade, use o Gerenciador de Grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta alterar IP se o Gerenciador de Grade estiver inacessível devido a um problema de configuração de rede, ou você estiver executando uma alteração de roteamento de rede de Grade e outras alterações de rede ao mesmo tempo.

Passos

1. Faça login no nó de administração principal:

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

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

2. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`
3. Insira a senha de provisionamento no prompt.

É apresentado o menu principal.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. No menu principal, selecione a opção para editar sub-redes para a rede de Grade (opção 4).



As alterações na Lista de sub-redes de rede de Grade são em toda a grade.

5. Escolha uma das seguintes opções:

- Adicione uma sub-rede inserindo este comando: `add CIDR`
- Exclua uma sub-rede inserindo este comando: `del CIDR`
- Defina a lista de sub-redes inserindo este comando: `set CIDR`



Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Você pode reduzir a quantidade de digitação necessária usando ""seta para cima"" para recuperar valores digitados anteriormente para o prompt de entrada atual e, em seguida, editá-los, se necessário.

A entrada de exemplo abaixo mostra a configuração de sub-redes para a Lista de sub-redes de rede de Grade:

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
 172.16.0.0/21
 172.17.0.0/21
 172.18.0.0/21
192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21 █
```

6. Quando estiver pronto, digite **q** para voltar à tela do menu principal. Suas alterações são mantidas até serem limpas ou aplicadas.
7. Escolha uma das seguintes opções:
 - Selecione a opção **5** para mostrar as edições na saída que estão isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída de exemplo abaixo:

```
-----  
Grid Network Subnet List (GNSL)  
-----  
add 172.30.0.0/21  
add 172.31.0.0/21  
del 172.16.0.0/21  
del 172.17.0.0/21  
del 172.18.0.0/21  
  
[ 172.30.0.0/21 ]  
[ 172.31.0.0/21 ]  
[ 192.168.0.0/21 ]  
  
Press Enter to continue
```

- Selecione a opção **6** para mostrar as edições na saída que exibem a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando a formatação strikethrough.

8. Selecione a opção **7** para validar todas as alterações faseadas.

Essa validação garante que as regras para redes Grid, Admin e Client sejam seguidas, como o uso de sub-redes sobrepostas.

9. Opcionalmente, selecione a opção **8** para guardar todas as alterações faseadas e voltar mais tarde para continuar a efetuar alterações.

Essa opção permite que você saia da ferramenta Change IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

10. Execute um dos seguintes procedimentos:

- Selecione a opção **9** se quiser limpar todas as alterações sem salvar ou aplicar a nova configuração de rede.
- Selecione a opção **10** se estiver pronto para aplicar alterações e provisionar a nova configuração de rede. Durante o provisionamento, a saída exibe o status à medida que as atualizações são aplicadas conforme mostrado na seguinte saída de amostra:

```
Generating new grid networking description file...  
  
Running provisioning...  
  
Updating grid network configuration on Name
```

11. Se você selecionou a opção **10** ao fazer alterações na rede de Grade, selecione uma das seguintes opções:

- **Apply:** Aplique as alterações imediatamente e reinicie automaticamente cada nó, se necessário.

Se a nova configuração de rede funcionar simultaneamente com a configuração de rede antiga sem alterações externas, você pode usar a opção **Apply** para uma alteração de configuração totalmente automatizada.

- **Stage:** Aplique as alterações na próxima vez que os nós forem reiniciados.

Se você precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, use a opção **stage**, encerre os nós afetados, faça as alterações de rede física necessárias e reinicie os nós afetados.



Se você usar a opção **stage**, será necessário reiniciar o nó o mais rápido possível após o preparo para minimizar as interrupções.

- **Cancelar:** Não faça alterações na rede neste momento.

Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o impactos do usuário. Selecionar **CANCEL** retorna ao menu principal e preserva as alterações para que você possa aplicá-las mais tarde.

Depois de aplicar ou preparar alterações, um novo pacote de recuperação é gerado como resultado da alteração da configuração da grade.

12. Se a configuração for interrompida devido a erros, as seguintes opções estarão disponíveis:

- Para cancelar o procedimento de alteração de IP e regressar ao menu principal, introduza **a**.
- Para tentar novamente a operação que falhou, digite **r**.
- Para continuar para a próxima operação, digite **c**.

A operação com falha pode ser tentada mais tarde selecionando a opção **10** (aplicar alterações) no menu principal. O procedimento de alteração de IP não será concluído até que todas as operações tenham sido concluídas com êxito.

- Se você teve que intervir manualmente (para reinicializar um nó, por exemplo) e está confiante de que a ação que a ferramenta acha que falhou foi realmente concluída com sucesso, digite **f** para marcá-lo como bem-sucedido e passar para a próxima operação.

13. Faça o download de um novo Pacote de recuperação do Gerenciador de Grade.

a. Selecione **MAINTENANCE > System > Recovery package**.

b. Introduza a frase-passe de provisionamento.



O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

Informações relacionadas

[Configurar endereços IP](#)

Altere endereços IP para todos os nós na grade

Se você precisar alterar o endereço IP da rede de Grade para todos os nós da grade, siga este procedimento especial. Você não pode fazer uma alteração de IP de rede de

grade em toda a grade usando o procedimento para alterar nós individuais.

O que você vai precisar

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

Para garantir que a grade seja iniciada com sucesso, você deve fazer todas as alterações de uma vez.



Este procedimento aplica-se apenas à rede de grelha. Não é possível usar este procedimento para alterar endereços IP nas redes Admin ou Client.

Se você quiser alterar os endereços IP e MTU para os nós apenas em um site, siga as [Alterar a configuração da rede do nó](#) instruções.

Passos

1. Planeje com antecedência as alterações que você precisa fazer fora da ferramenta Change IP, como alterações no DNS ou NTP, e alterações na configuração de logon único (SSO), se usado.



Se os servidores NTP existentes não estiverem acessíveis à grade nos novos endereços IP, adicione os novos servidores NTP antes de executar o procedimento Change-ip.



Se os servidores DNS existentes não estiverem acessíveis à grade nos novos endereços IP, adicione os novos servidores DNS antes de executar o procedimento Change-ip.



Se o SSO estiver habilitado para o seu sistema StorageGRID e quaisquer confianças de terceiros confiáveis tiverem sido configuradas usando endereços IP de nó de administrador (em vez de nomes de domínio totalmente qualificados, conforme recomendado), esteja preparado para atualizar ou reconfigurar essas confianças de terceiros confiáveis nos Serviços de Federação do ativo Directory (AD FS) imediatamente após você alterar endereços IP. Consulte as instruções para administrar o StorageGRID.



Se necessário, adicione a nova sub-rede para os novos endereços IP.

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. Inicie a ferramenta Change IP inserindo o seguinte comando: `change-ip`
4. Insira a senha de provisionamento no prompt.

É apresentado o menu principal. Por padrão, o `Selected nodes` campo é definido como `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

5. No menu principal, selecione **2** para editar informações sobre máscara de IP/sub-rede, gateway e MTU para todos os nós.

a. Selecione **1** para fazer alterações na rede de Grade.

Depois de fazer a seleção, o prompt mostra os nomes dos nós, o nome da rede da grade, o tipo de dados (IP/máscara, Gateway ou MTU) e os valores atuais.

Editar o endereço IP, o comprimento do prefixo, o gateway ou MTU de uma interface configurada por DHCP alterará a interface para estática. É apresentado um aviso antes de cada interface configurada pelo DHCP.

As interfaces configuradas como *fixed* não podem ser editadas.

a. Para definir um novo valor, introduza-o no formato apresentado para o valor atual.

b. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

Suas alterações são mantidas até serem limpas ou aplicadas.

6. Reveja as alterações selecionando uma das seguintes opções:

- **5**: Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são realçadas em verde (adições) ou vermelho (exclusões), como mostrado na saída do exemplo:

```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- 6: Mostra edições na saída que exibe a configuração completa. As alterações são realçadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando a formatação strikethrough. A exibição adequada depende do cliente terminal que suporta as seqüências de escape VT100 necessárias.

7. Selecione a opção 7 para validar todas as alterações.

Essa validação garante que as regras da rede de Grade, como não usar sub-redes sobrepostas, não sejam violadas.

Neste exemplo, a validação retornou erros.

```

Validating new networking configuration... FAILED.

DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

Neste exemplo, a validação passou.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

- Quando a validação passar, selecione **10** para aplicar a nova configuração de rede.
- Selecione **stage** para aplicar as alterações na próxima vez que os nós forem reiniciados.



Você deve selecionar **stage**. Não execute um reinício contínuo, manualmente ou selecionando **Apply** em vez de **stage**; a grade não será iniciada com êxito.

- Depois que as alterações estiverem concluídas, selecione **0** para sair da ferramenta Change IP (alterar IP).
- Encerre todos os nós simultaneamente.



Toda a grade deve ser desligada de uma só vez, de modo que todos os nós estejam inativos ao mesmo tempo.

- Faça as alterações de rede física ou virtual necessárias.
- Verifique se todos os nós da grade estão inativos.
- Potência em todos os nós.
- Assim que a grelha for iniciada com sucesso:
 - Se você adicionou novos servidores NTP, exclua os valores antigos do servidor NTP.
 - Se você adicionou novos servidores DNS, exclua os valores antigos do servidor DNS.
- Faça o download do novo Pacote de recuperação do Gerenciador de Grade.
 - Selecione **MAINTENANCE > System > Recovery package**.
 - Introduza a frase-passe de provisionamento.

Informações relacionadas

[Administrar o StorageGRID](#)

[Adicionar ou alterar listas de sub-rede na rede de Grade](#)

[Encerre o nó da grade](#)

Adicione interfaces ao nó existente

Linux: Adicione interfaces Admin ou Client a um nó existente

Siga estas etapas para adicionar uma interface na rede de administração ou na rede de cliente a um nó Linux depois de instalado.

Se você não configurou ADMIN_network_TARGET ou CLIENT_network_TARGET no arquivo de configuração do nó no host Linux durante a instalação, use este procedimento para adicionar a interface. Para obter mais informações sobre o arquivo de configuração do nó, consulte as instruções do seu sistema operacional Linux:

- [Instale o Red Hat Enterprise Linux ou CentOS](#)
- [Instale Ubuntu ou Debian](#)

Você executa este procedimento no servidor Linux que hospeda o nó que precisa da nova atribuição de rede, não dentro do nó. Este procedimento adiciona apenas a interface ao nó; ocorre um erro de validação se tentar especificar quaisquer outros parâmetros de rede.

Para fornecer informações de endereçamento, você deve usar a ferramenta alterar IP. [Alterar a configuração da rede do nó](#) Consulte .

Passos

1. Faça login no servidor Linux que hospeda o nó.
2. Edite o arquivo de configuração do nó `/etc/storagegrid/nodes/node-name.conf`:



Não especifique quaisquer outros parâmetros de rede, ou um erro de validação resultará.

- a. Adicione uma entrada para o novo destino de rede. Por exemplo:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Opcional: Adicione uma entrada para o endereço MAC. Por exemplo:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Execute o comando Node Validate:

```
sudo storagegrid node validate node-name
```

4. Resolva todos os erros de validação.

5. Execute o comando node reload:

```
sudo storagegrid node reload node-name
```

Linux: Adicione interfaces de tronco ou acesso a um nó

Você pode adicionar interfaces de tronco ou acesso extras a um nó Linux depois que ele foi instalado. As interfaces adicionadas são exibidas na página interfaces VLAN e na página grupos HA.

O que você vai precisar

- Você tem acesso às instruções para instalar o StorageGRID em sua plataforma Linux.
 - [Instale o Red Hat Enterprise Linux ou CentOS](#)
 - [Instale Ubuntu ou Debian](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem permissões de acesso específicas.



Não tente adicionar interfaces a um nó enquanto uma atualização de software, procedimento de recuperação ou procedimento de expansão estiver ativo.

Sobre esta tarefa

Siga estas etapas para adicionar uma ou mais interfaces extras a um nó Linux após a instalação do nó. Por exemplo, você pode querer adicionar uma interface de tronco a um Admin ou Gateway Node, para que você possa usar interfaces VLAN para segregar o tráfego que pertence a diferentes aplicativos ou locatários. Ou, talvez você queira adicionar uma interface de acesso para usar em um grupo de alta disponibilidade (HA).

Se você adicionar uma interface de tronco, deverá configurar uma interface de VLAN no StorageGRID. Se

Se você adicionar uma interface de acesso, poderá adicionar a interface diretamente a um grupo HA; não será necessário configurar uma interface VLAN.

O nó fica indisponível por um breve período de tempo quando você adiciona interfaces. Você deve executar este procedimento em um nó de cada vez.

Passos

1. Faça login no servidor Linux que hospeda o nó.
2. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Adicione uma entrada ao arquivo para especificar o nome e, opcionalmente, a descrição de cada interface extra que você deseja adicionar ao nó. Use este formato.

```
INTERFACES_TARGET_nnnn=value
```

Para *nnnn*, especifique um número exclusivo para cada INTERFACES_TARGET entrada que você está adicionando.

Para *value*, especifique o nome da interface física no host bare-metal. Em seguida, opcionalmente, adicione uma vírgula e forneça uma descrição da interface, que é exibida na página interfaces VLAN e na página grupos HA.

Por exemplo:

```
INTERFACES_TARGET_01=ens256, Trunk
```



Não especifique quaisquer outros parâmetros de rede, ou um erro de validação resultará.

4. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó:

```
sudo storagegrid node validate node-name
```

Solucione quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

5. Execute o seguinte comando para atualizar a configuração do nó:

```
sudo storagegrid node reload node-name
```

Depois de terminar

- Se você tiver adicionado uma ou mais interfaces de tronco, vá para [Configurar interfaces VLAN](#) para configurar uma ou mais interfaces VLAN para cada nova interface pai.
- Se você adicionou uma ou mais interfaces de acesso, acesse [configurar grupos de alta disponibilidade](#) para adicionar as novas interfaces diretamente aos grupos de HA.

VMware: Adicione interfaces de tronco ou acesso a um nó

Você pode adicionar um tronco ou uma interface de acesso a um nó da VM depois que o nó tiver sido instalado. As interfaces adicionadas são exibidas na página interfaces VLAN e na página grupos HA.

O que você vai precisar

- Você tem acesso às instruções para instalar o StorageGRID em sua plataforma VMware.

Instale o VMware

- Você configurou o StorageGRID 11,6.
- Você tem máquinas virtuais Admin Node e Gateway Node VMware.
- Você tem uma sub-rede de rede que não está sendo usada como rede Grid, Admin ou Client.
- Você tem o `Passwords.txt` arquivo.
- Você tem permissões de acesso específicas.



Não tente adicionar interfaces a um nó enquanto uma atualização de software, procedimento de recuperação ou procedimento de expansão estiver ativo.

Sobre esta tarefa

Siga estas etapas para adicionar uma ou mais interfaces extras a um nó VMware depois que o nó tiver sido instalado. Por exemplo, você pode querer adicionar uma interface de tronco a um Admin ou Gateway Node, para que você possa usar interfaces VLAN para segregar o tráfego que pertence a diferentes aplicativos ou locatários. Ou você pode querer adicionar uma interface de acesso para usar em um grupo de alta disponibilidade (HA).

Se você adicionar uma interface de tronco, deverá configurar uma interface de VLAN no StorageGRID. Se você adicionar uma interface de acesso, poderá adicionar a interface diretamente a um grupo HA; não será necessário configurar uma interface VLAN.

O nó pode estar indisponível por um breve período de tempo quando você adiciona interfaces.

Passos

1. No vCenter, adicione um novo adaptador de rede (tipo VMXNET3) a uma VM Admin Node e Gateway Node. Selecione as caixas de verificação **Connected** e **Connect at Power On**.

Network adapter 4 *	CLIENT683_old_vlan	Connected
Status	<input checked="" type="checkbox"/> Connect At Power On	
Adapter Type	VMXNET 3	
DirectPath I/O	<input checked="" type="checkbox"/> Enable	

2. Use SSH para fazer login no Admin Node ou Gateway Node.
3. Utilize `ip link show` para confirmar que foi detetada a nova interface de rede `ens256`.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Depois de terminar

- Se você tiver adicionado uma ou mais interfaces de tronco, vá para [Configurar interfaces VLAN](#) para configurar uma ou mais interfaces VLAN para cada nova interface pai.
- Se você adicionou uma ou mais interfaces de acesso, acesse [configurar grupos de alta disponibilidade](#) para adicionar as novas interfaces diretamente aos grupos de HA.

Configurar servidores DNS

Você pode adicionar, remover e atualizar servidores DNS (sistema de nomes de domínio), para que você possa usar nomes de host FQDN (nome de domínio totalmente qualificado) em vez de endereços IP.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter os endereços IP dos servidores DNS para configurar.

Especificar informações do servidor DNS permite que você use nomes de host de nome de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações de e-mail ou SNMP e AutoSupport. É recomendável especificar pelo menos dois servidores DNS.



Forneça entre dois a seis endereços IP para servidores DNS. Em geral, selecione servidores DNS que cada site pode acessar localmente no caso de a rede ser aterrissada. Isso é para garantir que um site islanded continua a ter acesso ao serviço DNS. Depois de configurar a lista de servidores DNS em toda a grade, você pode [Personalize ainda mais a lista de servidores DNS para cada nó](#).

Se as informações do servidor DNS forem omitidas ou configuradas incorretamente, um alarme DNST será acionado no serviço SSM de cada nó da grade. O alarme é apagado quando o DNS está configurado corretamente e as novas informações do servidor atingiram todos os nós da grade.

Passos

1. Selecione **MAINTENANCE > Network > DNS Servers**.
2. Na seção servidores, adicione atualizações ou remova entradas do servidor DNS, conforme necessário.

A prática recomendada é especificar pelo menos dois servidores DNS por site. Você pode especificar até seis servidores DNS.

3. Clique em **Salvar**.

Modifique a configuração DNS para um nó de grade único

Em vez de configurar o DNS (Domain Name System) globalmente para toda a implantação, você pode executar um script para configurar o DNS de forma diferente para cada nó de grade.

Em geral, você deve usar a opção **MAINTENANCE Network DNS Servers** no Gerenciador de Grade para configurar servidores DNS. Use o script a seguir somente se você precisar usar servidores DNS diferentes para diferentes nós de grade.

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

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
 - e. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
 - f. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
2. Faça login no nó que deseja atualizar com uma configuração DNS personalizada: `ssh node_IP_address`
3. Execute o script de configuração DNS: `setup_resolv.rb`.

O script responde com a lista de comandos suportados.

Tool to modify external name servers

available commands:

```
add search <domain>
    add a specified domain to search list
    e.g.> add search netapp.com
remove search <domain>
    remove a specified domain from list
    e.g.> remove search netapp.com
add nameserver <ip>
    add a specified IP address to the name server list
    e.g.> add nameserver 192.0.2.65
remove nameserver <ip>
    remove a specified IP address from list
    e.g.> remove nameserver 192.0.2.65
remove nameserver all
    remove all nameservers from list
save
    write configuration to disk and quit
abort
    quit without saving changes
help
    display this help message
```

Current list of name servers:

```
192.0.2.64
```

Name servers inherited from global DNS configuration:

```
192.0.2.126
```

```
192.0.2.127
```

Current list of search entries:

```
netapp.com
```

```
Enter command [ `add search <domain>|remove search <domain>|add
nameserver <ip>` ]
```

```
                [ `remove nameserver <ip>|remove nameserver
all|save|abort|help` ]
```

4. Adicione o endereço IPv4 de um servidor que fornece serviço de nome de domínio para sua rede: `add <nameserver IP_address>`
5. Repita o `add nameserver` comando para adicionar servidores de nomes.
6. Siga as instruções conforme solicitado para outros comandos.
7. Salve suas alterações e saia do aplicativo: `save`
8. feche o shell de comando no servidor: `exit`
9. Para cada nó de grade, repita as etapas de [iniciar sessão no nó](#) até [fechando o shell de comando](#).
10. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do

agente SSH. Introduza: `ssh-add -D`

Configurar servidores NTP

Você pode adicionar, atualizar ou remover servidores NTP (Network Time Protocol) para garantir que os dados sejam sincronizados com precisão entre nós de grade em seu sistema StorageGRID.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Tem de ter a permissão Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento.
- Você deve ter os endereços IPv4 dos servidores NTP para configurar.

Sobre esta tarefa

O sistema StorageGRID usa o protocolo de tempo de rede (NTP) para sincronizar o tempo entre todos os nós de grade na grade.

Em cada local, pelo menos dois nós no sistema StorageGRID recebem a função NTP principal. Eles sincronizam com um mínimo sugerido de quatro, e um máximo de seis, fontes de tempo externas e entre si. Cada nó no sistema StorageGRID que não é um nó NTP primário atua como um cliente NTP e sincroniza com esses nós NTP primários.

Os servidores NTP externos conectam-se aos nós aos quais você atribuiu funções primárias NTP anteriormente. Por esse motivo, é recomendável especificar pelo menos dois nós com funções NTP primárias.



Certifique-se de que pelo menos dois nós em cada local possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um local puder alcançar as fontes NTP, problemas de tempo ocorrerão se esse nó cair. Além disso, a designação de dois nós por local como fontes primárias de NTP garante um tempo preciso se um local for isolado do resto da grade.

Os servidores NTP externos especificados devem usar o protocolo NTP. Você deve especificar referências de servidor NTP do estrato 3 ou melhor para evitar problemas com a deriva de tempo.



Ao especificar a fonte NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

"Limite de suporte para configurar o serviço de tempo do Windows para ambientes de alta precisão"

Se você encontrar problemas com a estabilidade ou disponibilidade dos servidores NTP originalmente especificados durante a instalação, você pode atualizar a lista de fontes NTP externas que o sistema StorageGRID usa adicionando servidores adicionais ou atualizando ou removendo servidores existentes.

Passos

1. Selecione **MAINTENANCE > Network > NTP Servers**.
2. Na seção servidores, adicione atualizações ou remova entradas do servidor NTP, conforme necessário.

Você deve incluir pelo menos 4 servidores NTP e pode especificar até 6 servidores.

3. Na caixa de texto **frase-passe de provisionamento**, introduza a frase-passe de provisionamento do sistema StorageGRID e clique em **Guardar**.

O estado do procedimento é apresentado na parte superior da página. A página é desativada até que as atualizações de configuração estejam concluídas.



Se todos os seus servidores NTP falharem no teste de conexão depois de salvar os novos servidores NTP, não prossiga. Entre em Contato com o suporte técnico.

Restaurar a conectividade de rede para nós isolados

Em certas circunstâncias, como alterações de endereço IP em todo o site ou grade, um ou mais grupos de nós podem não ser capazes de entrar em Contato com o resto da grade.

No Gerenciador de Grade (**SUPPORT Tools Grid topology**), se um nó estiver cinza ou se um nó estiver azul com muitos de seus serviços mostrando um status diferente de Running, você deve verificar se há isolamento de nó.

The screenshot shows the 'Grid Topology' interface. On the left is a tree view of the grid structure, including 'Grid1', 'Site1', and several nodes like 'abrian-g1', 'abrian-s1', 'abrian-s2', and 'abrian-s3'. On the right, the 'Overview' tab is selected, showing 'Main' and 'Overview: SSM (abrian-g1) - Services'. The operating system is 'Linux 4.9.0-3-amd64'. Below this is a table of services and a table of packages.

Service	Version	Status	Threads	Load	Memory
ADE Exporter Service	11.1.0-20171214.1441.c29e2f8	Running	11	0.011 %	7.87 MB
Connection Load Balancer (CLB)	11.1.0-20180120.0111.02137fe	Running	61	0.07 %	39.3 MB
Dynamic IP Service	11.1.0-20180123.1919.deeeba7.abrian	Not Running	0	0 %	0 B
Nginx Service	1.10.3-1+deb9u1	Running	5	0.002 %	20 MB
Node Exporter Service	0.13.0+ds-1+b2	Running	5	0 %	8.58 MB
Persistence Service	11.1.0-20180123.1919.deeeba7.abrian	Running	6	0.064 %	17.1 MB
Server Manager	11.1.0-20171214.1441.c29e2f8	Running	4	2.116 %	18.7 MB
Server Status Monitor (SSM)	11.1.0-20180120.0111.02137fe	Running	61	0.288 %	45.8 MB
System Logging	3.8.1-10	Running	3	0.006 %	8.27 MB
Time Synchronization	1:4.2.8p10+dfsg-3+deb9u1	Running	2	0.007 %	4.54 MB

Package	Installed	Version
storage-grid-release	Installed	11.1.0-20180123.1919.deeeba7.abrian

Algumas das consequências de ter nós isolados incluem o seguinte:

- Se vários nós estiverem isolados, talvez você não consiga entrar ou acessar o Gerenciador de Grade.
- Se vários nós estiverem isolados, o uso do storage e os valores de cota mostrados no Dashboard do Tenant Manager podem estar desatualizados. Os totais serão atualizados quando a conectividade de rede for restaurada.

Para resolver o problema de isolamento, você executa um utilitário de linha de comando em cada nó isolado ou em um nó em um grupo (todos os nós em uma sub-rede que não contém o nó Admin principal) que é isolado da grade. O utilitário fornece aos nós o endereço IP de um nó não isolado na grade, o que permite que o nó isolado ou grupo de nós entre em Contato com toda a grade novamente.



Se o sistema de nomes de domínio multicast (mDNS) estiver desativado nas redes, o utilitário de linha de comando pode ter de ser executado em cada nó isolado.

1. Acesse o nó e `/var/local/log/dynip.log` verifique se há mensagens de isolamento.

Por exemplo:

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action may be required.
```

Se você estiver usando o console VMware, ele conterá uma mensagem informando que o nó pode estar isolado.

Nas implantações Linux, as mensagens de isolamento aparecerão nos `/var/log/storagegrid/node/<nodename>.log` arquivos.

2. Se as mensagens de isolamento forem recorrentes e persistentes, execute o seguinte comando:

```
add_node_ip.py <address>
```

```
`<address>`Onde está o endereço IP de um nó remoto que está conetado à
grade.
```

```
# /usr/sbin/add_node_ip.py 10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Verifique o seguinte para cada nó que foi isolado anteriormente:

- Os serviços do nó foram iniciados.
- O status do serviço IP dinâmico é "em execução" depois de executar o `storagegrid-status` comando.
- Na árvore topologia de Grade, o nó não aparece mais desconetado do resto da grade.



Se a execução do `add_node_ip.py` comando não resolver o problema, pode haver outros problemas de rede que precisam ser resolvidos.

Procedimentos de nível de host e middleware

Alguns procedimentos de manutenção são específicos para implantações Linux ou VMware do StorageGRID, ou são específicos para outros componentes da solução

StorageGRID.

Linux: Migrar o nó de grade para o novo host

Você pode migrar os nós do StorageGRID de um host Linux para outro para executar a manutenção do host (como patches e reinicialização do sistema operacional) sem afetar a funcionalidade ou a disponibilidade da sua grade.

Você migra um ou mais nós de um host Linux (o "host de origem") para outro host Linux (o "host de destino"). O host de destino deve ter sido preparado anteriormente para uso no StorageGRID.



Você pode usar este procedimento somente se você planejou sua implantação do StorageGRID para incluir suporte à migração.

Para migrar um nó de grade para um novo host, ambas as condições a seguir devem ser verdadeiras:

- O storage compartilhado é usado para todos os volumes de storage por nó
- As interfaces de rede têm nomes consistentes entre os hosts



Em uma implantação de produção, não execute mais de um nó de storage em um único host. O uso de um host dedicado para cada nó de storage fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados no mesmo host. No entanto, se você tiver vários nós do mesmo tipo (dois nós de Gateway, por exemplo), não instale todas as instâncias no mesmo host.

Para obter mais informações, consulte "requisitos de migração de nós" nas instruções de instalação do StorageGRID para o seu sistema operacional Linux.

Informações relacionadas

[Implante novos hosts Linux](#)

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

Linux: Nó de exportação do host de origem

Encerre o nó da grade e exporte-o do host Linux de origem.

Execute o seguinte comando no host Linux de origem.

1. Obtenha o status de todos os nós atualmente em execução no host de origem.

```
sudo storagegrid node status all
```

```
Name Config-State Run-State
```

```
DC1-ADM1 Configured Running
```

DC1-ARC1 Configured Running

DC1-GW1 Configured Running

DC1-S1 Configured Running

DC1-S2 Configured Running

DC1-S3 Configured Running

2. Identifique o nome do nó que deseja migrar e pare-o se o estado de execução for Running.

```
sudo storagegrid node stop DC1-S3
```

Stopping node DC1-S3

Waiting up to 630 seconds for node shutdown

3. Exporte o nó do host de origem.

```
sudo storagegrid node export DC1-S3
```

Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.

Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you want to import it again.

4. Tome nota import command suggested in the output of the `export do comando.

Você executará esse comando no host de destino na próxima etapa.

Linux: Importar nó no host de destino

Depois de exportar o nó do host de origem, você importa e valida o nó no host Linux de destino. A validação confirma que o nó tem acesso aos mesmos dispositivos de interface de rede e armazenamento de bloco que tinha no host de origem.

Execute o seguinte comando no host Linux de destino.

1. Importe o nó no host de destino.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'

2. Valide a configuração do nó no novo host.

```
sudo storagegrid node validate DC1-S3
```

```
Confirming existence of node DC1-S3... PASSED
```

```
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-S3... PASSED
```

```
Checking for duplication of unique values... PASSED
```

3. Se ocorrerem erros de validação, solucione-os antes de iniciar o nó migrado.

Para obter informações sobre solução de problemas, consulte as instruções de instalação do StorageGRID para seu sistema operacional Linux.

Informações relacionadas

[Instale o Red Hat Enterprise Linux ou CentOS](#)

[Instale Ubuntu ou Debian](#)

Linux: Inicie o nó migrado

Depois de validar o nó migrado, você inicia o nó executando um comando no host Linux de destino.

Passos

1. Inicie o nó no novo host.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. No Gerenciador de Grade, verifique se o status do nó está verde sem alarmes levantados contra ele.



Verificar se o status do nó está verde garante que o nó migrado tenha reiniciado e se juntado novamente à grade. Se o status não estiver verde, não migre nenhum nó adicional para que você não tenha mais de um nó fora de serviço.

Se você não conseguir acessar o Gerenciador de Grade, aguarde 10 minutos e execute o seguinte comando:

```
sudo storagegrid node status node-name
```

Confirme se o nó migrado tem um Estado de execução de `Running`.

Manutenção do Archive Node para middleware TSM

Os nós de arquivamento podem ser configurados para direcionar a fita por meio de um

servidor middleware TSM ou a nuvem por meio da API S3. Uma vez configurado, o destino de um nó de arquivo não pode ser alterado.

Se o servidor que hospeda o nó de arquivo falhar, substitua o servidor e siga o procedimento de recuperação apropriado.

Falha com dispositivos de armazenamento de arquivo

Se você determinar que há uma falha no dispositivo de armazenamento de arquivos que o nó de arquivamento está acessando por meio do Gerenciador de armazenamento Tivoli (TSM), coloque o nó de arquivamento off-line para limitar o número de alarmes exibidos no sistema StorageGRID. Em seguida, você pode usar as ferramentas administrativas do servidor TSM ou do dispositivo de armazenamento, ou ambos, para diagnosticar e resolver o problema.

Coloque o componente alvo offline

Antes de realizar qualquer manutenção do servidor de middleware TSM que possa resultar na indisponibilidade do Archive Node, coloque o componente Target offline para limitar o número de alarmes que são acionados se o servidor de middleware TSM ficar indisponível.

O que você vai precisar

Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Target > Configuration > Main**.
3. Altere o valor do Tivoli Storage Manager State para **Offline** e clique em **Apply Changes**.
4. Após a conclusão da manutenção, altere o valor do Tivoli Storage Manager State para **Online** e clique em **Apply Changes**.

Ferramentas administrativas do Tivoli Storage Manager

A ferramenta dsmadm é o console administrativo do servidor de middleware TSM que está instalado no nó de Arquivo. Você pode acessar a ferramenta digitando `dsmadm` na linha de comando do servidor. Faça login no console administrativo usando o mesmo nome de usuário administrativo e senha configurados para o serviço ARC.

O `tsmquery.rb` script foi criado para gerar informações de status do dsmadm de forma mais legível. Você pode executar este script inserindo o seguinte comando na linha de comando do nó de Arquivo:

```
/usr/local/arc/tsmquery.rb status
```

Para obter mais informações sobre o console administrativo do TSM dsmadm, consulte *Tivoli Storage Manager for Linux: Administrators Reference*.

Objeto permanentemente indisponível

Quando o Archive Node solicita um objeto do servidor Tivoli Storage Manager (TSM) e a recuperação falha, o Archive Node tenta novamente a solicitação após um intervalo de 10 segundos. Se o objeto estiver permanentemente indisponível (por exemplo, porque o objeto está corrompido na fita), a API TSM não tem como indicar isso para o nó de arquivo, portanto, o nó de arquivo continua a tentar novamente a solicitação.

Quando esta situação ocorre, um alarme é acionado e o valor continua a aumentar. Para ver o alarme, selecione **support > Tools > Grid topology**. Em seguida, selecione **Archive Node > ARC > Retrieve >**

Request Failures.

Se o objeto estiver permanentemente indisponível, você deverá identificar o objeto e cancelar manualmente a solicitação do nó de arquivo conforme descrito no procedimento, [Determinar se os objetos estão permanentemente indisponíveis](#).

Uma recuperação também pode falhar se o objeto estiver temporariamente indisponível. Neste caso, as solicitações de recuperação subsequentes devem eventualmente ser bem-sucedidas.

Se o sistema StorageGRID estiver configurado para usar uma regra ILM que cria uma cópia de objeto único e essa cópia não puder ser recuperada, o objeto será perdido e não poderá ser recuperado. No entanto, você ainda deve seguir o procedimento para determinar se o objeto está permanentemente indisponível para "limpar" o sistema StorageGRID, para cancelar a solicitação do nó de Arquivo e para purgar metadados para o objeto perdido.

Determinar se os objetos estão permanentemente indisponíveis

Você pode determinar se os objetos estão permanentemente indisponíveis fazendo uma solicitação usando o console administrativo do TSM.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

Este exemplo é fornecido apenas para suas informações; este procedimento não pode ajudá-lo a identificar todas as condições de falha que podem resultar em objetos indisponíveis ou volumes de fita. Para obter informações sobre a administração do TSM, consulte a documentação do TSM Server.

Passos

1. Faça login em um nó Admin:
 - a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Identifique o objeto ou objetos que não puderam ser recuperados pelo nó de arquivo:
 - a. Vá para o diretório que contém os arquivos de log de auditoria: `cd /var/local/audit/export`

O arquivo de log de auditoria ativo é chamado `audit.log`. Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`. Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

- b. Procure no ficheiro de registo de auditoria relevantes mensagens que indiquem que não foi possível obter um objeto arquivado. Por exemplo, digite: `grep ARCE audit.log | less -n`

Quando um objeto não pode ser recuperado de um nó de arquivo, a mensagem de AUDITORIA ARCE (Archive Object Retrieve End) exibe ARUN (archive middleware unavailable) ou GERR (erro geral) no campo de resultados. A linha de exemplo a seguir do log de auditoria mostra que a mensagem ARCE terminou com a EXECUÇÃO de resultado para CBID 498D8A1F681F05B3.

```
[AUDT: [CBID (UI64) : 0x498D8A1F681F05B3] [VLID (UI64) : 20091127] [RSLT (FC32) : ARUN] [AVER (UI32) : 7]
[ATIM (UI64) : 1350613602969243] [ATYP (FC32) : ARCE] [ANID (UI32) : 13959984] [AMID (FC32) : ARCI]
[ATID (UI64) : 4560349751312520631]]
```

Para obter mais informações, consulte as instruções para entender as mensagens de auditoria.

- c. Registre o CBID de cada objeto que teve uma falha de solicitação.

Você também pode querer gravar as seguintes informações adicionais usadas pelo TSM para identificar objetos salvos pelo nó de arquivo:

- **Nome do espaço de arquivo:** Equivalente ao ID do nó de arquivo. Para encontrar o ID do nó de arquivo, selecione **support > Tools > Grid topology**. Em seguida, selecione **Archive Node > ARC > Target > Overview**.
- **Nome de alto nível:** Equivalente ao ID de volume atribuído ao objeto pelo nó de arquivo. O ID do volume assume a forma de uma data (por exemplo, 20091127) e é gravado como o VLID do objeto em mensagens de auditoria de arquivo.
- **Nome de nível baixo:** Equivalente ao CBID atribuído a um objeto pelo sistema StorageGRID.

- d. Faça logout do shell de comando: `exit`

3. Verifique o servidor TSM para ver se os objetos identificados na etapa 2 estão permanentemente indisponíveis:

- a. Faça login no console administrativo do servidor TSM: `dsmadm`

Use o nome de usuário administrativo e a senha configurados para o serviço ARC. Introduza o nome de utilizador e a palavra-passe no Gestor de grelha. (Para ver o nome de utilizador, selecione **support > Tools > Grid topology**. Em seguida, selecione **Archive Node > ARC > Target > Configuration**.)

- b. Determine se o objeto está permanentemente indisponível.

Por exemplo, você pode pesquisar no log de atividade do TSM um erro de integridade de dados para esse objeto. O exemplo a seguir mostra uma pesquisa do log de atividades para o dia passado para um objeto com CBID . 498D8A1F681F05B3

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

Dependendo da natureza do erro, o CBID pode não ser registrado no log de atividades do TSM. Talvez seja necessário pesquisar no log outros erros do TSM no momento da falha da solicitação.

- c. Se uma fita inteira estiver permanentemente indisponível, identifique os CBIDs para todos os objetos armazenados nesse volume: `query content TSM_Volume_Name`

``TSM_Volume_Name``Onde está o nome TSM para a fita indisponível. O seguinte é um exemplo da saída para este comando:

```
> query content TSM-Volume-Name
Node Name      Type Filespace  FSID Client's Name for File Name
-----
DEV-ARC-20    Arch /19130020   216 /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020   216 /20081201/ F1D7FBC2B4B0779E
```

O `Client's Name for File Name` é o mesmo que o ID do volume do nó de arquivo (ou TSM ""nome de alto nível"") seguido pelo CBID do objeto (ou TSM ""nome de baixo nível""). Ou seja, o `Client's Name for File Name` toma a forma `/Archive Node volume ID /CBID`. Na primeira linha da saída de exemplo, o `Client's Name for File Name` é `/20081201/C1D172940E6C7E12`.

Lembre-se também de que o `Filespace` é o ID do nó do nó de arquivo.

Você precisará do CBID de cada objeto armazenado no volume e do ID do nó do nó de arquivo para cancelar a solicitação de recuperação.

4. Para cada objeto que está permanentemente indisponível, cancele a solicitação de recuperação e emita um comando para informar o sistema StorageGRID de que a cópia do objeto foi perdida:



Use o console ADE com cuidado. Se o console for usado incorretamente, é possível interromper as operações do sistema e corromper os dados. Introduza os comandos cuidadosamente e utilize apenas os comandos documentados neste procedimento.

- a. Se você ainda não estiver conectado ao nó de arquivamento, faça login da seguinte forma:

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

- b. Acesse à consola ADE do serviço ARC: `telnet localhost 1409`

- c. Cancelar a solicitação para o objeto: `/proc/BRTR/cancel -c CBID`

``CBID``Onde está o identificador do objeto que não pode ser recuperado do TSM.

Se as únicas cópias do objeto estiverem em fita, a solicitação de "recuperação em massa" será cancelada com uma mensagem ""1 solicitações canceladas". Se houver cópias do objeto em outro

lugar do sistema, a recuperação do objeto é processada por um módulo diferente, de modo que a resposta à mensagem seja "O solicitações canceladas".

- d. Emita um comando para notificar o sistema StorageGRID de que uma cópia de objeto foi perdida e que uma cópia adicional deve ser feita: `/proc/CMSI/Object_Lost CBID node_ID`

```
`CBID`Onde está o identificador do objeto que não pode ser recuperado do servidor TSM `node_ID` e é o ID do nó do nó de arquivo onde a recuperação falhou.
```

Você deve inserir um comando separado para cada cópia de objeto perdido: Inserir um intervalo de CBIDs não é suportado.

Na maioria dos casos, o sistema StorageGRID começa imediatamente a fazer cópias adicionais de dados de objeto para garantir que a política de ILM do sistema seja seguida.

No entanto, se a regra ILM para o objeto especificar que apenas uma cópia será feita e essa cópia agora foi perdida, o objeto não pode ser recuperado. Nesse caso, executar o `Object_Lost` comando limpa os metadados do objeto perdido do sistema StorageGRID.

Quando o `Object_Lost` comando for concluído com êxito, a seguinte mensagem é retornada:

```
CLOC_LOST_ANS returned result `SUCS`
```

+



O `/proc/CMSI/Object_Lost` comando só é válido para objetos perdidos que são armazenados em nós de arquivo.

- a. Saia da consola ADE: `exit`
 - b. Terminar sessão no nó de arquivo: `exit`
5. Repor o valor de falhas de pedido no sistema StorageGRID:
 - a. Acesse a **Archive Node > ARC > Retrieve > Configuration** e selecione **Reset Request Failure Count**.
 - b. Clique em **aplicar alterações**.

Informações relacionadas

[Administrar o StorageGRID](#)

[Rever registos de auditoria](#)

VMware: Configure a máquina virtual para reinicialização automática

Se a máquina virtual não reiniciar depois que o VMware vSphere Hypervisor for reiniciado, talvez seja necessário configurar a máquina virtual para reinicialização automática.

Você deve executar este procedimento se notar que uma máquina virtual não reinicia enquanto estiver recuperando um nó de grade ou executando outro procedimento de manutenção.

Passos

1. Na árvore Cliente do VMware vSphere, selecione a máquina virtual que não foi iniciada.
2. Clique com o botão direito do rato na máquina virtual e selecione **ligar**.
3. Configure o VMware vSphere Hypervisor para reiniciar a máquina virtual automaticamente no futuro.

Procedimentos do nó de grade

Talvez seja necessário executar procedimentos em um nó de grade específico. Embora você possa executar alguns desses procedimentos no Gerenciador de Grade, a maioria dos procedimentos exige que você acesse o Gerenciador de servidor a partir da linha de comando do nó.

O Gerenciador de servidores é executado em cada nó de grade para supervisionar o início e a parada dos serviços e garantir que os serviços se juntem e saiam do sistema StorageGRID. O Gerenciador de servidores também monitora os serviços em cada nó de grade e tentará reiniciar automaticamente quaisquer serviços que relatem falhas.



Você deve acessar o Server Manager somente se o suporte técnico o tiver direcionado para isso.



Você deve fechar a sessão de shell de comando atual e fazer logout depois de terminar com o Gerenciador de servidor. Introduza: `exit`

Exibir o status e a versão do Server Manager

Para cada nó de grade, você pode exibir o status atual e a versão do Server Manager em execução nesse nó de grade. Você também pode obter o status atual de todos os serviços executados nesse nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Veja o status atual do Server Manager em execução no nó da grade: **`service servermanager status`**

O status atual do Server Manager em execução no nó da grade é relatado (em execução ou não). Se o status do Gerenciador de servidor for `running`, a hora em que ele foi executado desde a última vez em que foi iniciado é listada. Por exemplo:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Veja a versão atual do Server Manager em execução em um nó de grade: **`service servermanager version`**

A versão atual é listada. Por exemplo:

```
11.1.0-20180425.1905.39c9493
```

4. Faça logout do shell de comando: **`exit`**

Ver o estado atual de todos os serviços

Você pode visualizar o status atual de todos os serviços executados em um nó de grade a qualquer momento.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Veja o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Por exemplo, a saída para o nó de administração principal mostra o status atual dos serviços AMS, CMN e NMS como em execução. Essa saída é atualizada imediatamente se o status de um serviço mudar.

Host Name	190-ADM1	
IP Address		
Operating System Kernel	4.9.0	Verified
Operating System Environment	Debian 9.4	Verified
StorageGRID Webscale Release	11.1.0	Verified
Networking		Verified
Storage Subsystem		Verified
Database Engine	5.5.9999+default	Running
Network Monitoring	11.1.0	Running
Time Synchronization	1:4.2.8p10+dfsg	Running
ams	11.1.0	Running
cmn	11.1.0	Running
nms	11.1.0	Running
ssm	11.1.0	Running
mi	11.1.0	Running
dynip	11.1.0	Running
nginx	1.10.3	Running
tomcat	8.5.14	Running
grafana	4.2.0	Running
mgmt api	11.1.0	Running
prometheus	1.5.2+ds	Running
persistence	11.1.0	Running
ade exporter	11.1.0	Running
attrDownPurge	11.1.0	Running
attrDownSampl	11.1.0	Running
attrDownSamp2	11.1.0	Running
node exporter	0.13.0+ds	Running

- Volte para a linha de comando, pressione **Ctrl** * **C**.*
- Opcionalmente, exiba um relatório estático para todos os serviços executados no nó da grade:
`/usr/local/servermanager/reader.rb`

Este relatório inclui as mesmas informações que o relatório continuamente atualizado, mas não é atualizado se o status de um serviço for alterado.

- Faça logout do shell de comando: `exit`

Inicie o Server Manager e todos os serviços

Talvez seja necessário iniciar o Server Manager, que também inicia todos os serviços no nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Iniciar o Server Manager em um nó de grade onde ele já está sendo executado resulta em uma reinicialização do Server Manager e de todos os serviços no nó de grade.

Passos

- Faça login no nó da grade:
 - Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Iniciar o Gestor de servidor: `service servermanager start`

3. Faça logout do shell de comando: `exit`

Reinicie o Server Manager e todos os serviços

Talvez seja necessário reiniciar o gerenciador de servidor e todos os serviços em execução em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Reinicie o Server Manager e todos os serviços no nó de grade: `service servermanager restart`

O Gerenciador de servidores e todos os serviços no nó de grade são interrompidos e reiniciados.



Utilizar o `restart` comando é o mesmo que utilizar o `stop` comando seguido do `start` comando.

3. Faça logout do shell de comando: `exit`

Pare o Server Manager e todos os serviços

O Server Manager destina-se a ser executado em todos os momentos, mas pode ser necessário parar o Server Manager e todos os serviços executados em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

a. Introduza o seguinte comando: `ssh admin@grid_node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Stop Server Manager e todos os serviços em execução no nó de grade: `service servermanager stop`

O Gerenciador de servidores e todos os serviços executados no nó de grade são terminados graciosamente. Os serviços podem levar até 15 minutos para serem encerrados.

3. Faça logout do shell de comando: `exit`

Ver o estado atual do serviço

Você pode visualizar o status atual de um serviço em execução em um nó de grade a qualquer momento.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Exibir o status atual de um serviço em execução em um nó de grade: "**Service servicename status** o status atual do serviço solicitado em execução no nó de grade é relatado (em execução ou não). Por exemplo:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Faça logout do shell de comando: **exit**

Pare o serviço

Alguns procedimentos de manutenção exigem que você pare um único serviço enquanto mantém outros serviços no nó da grade em execução. Apenas pare os serviços individuais quando for direcionado para o fazer através de um procedimento de manutenção.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Quando você usa essas etapas para "parar administrativamente" um serviço, o Gerenciador de servidor não reiniciará automaticamente o serviço. Você deve iniciar o único serviço manualmente ou reiniciar o Server Manager.

Se necessitar de parar o serviço LDR num nó de armazenamento, tenha em atenção que poderá demorar algum tempo a parar o serviço se existirem ligações ativas.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Parar um serviço individual: `service servicename stop`

Por exemplo:

```
service ldr stop
```



Os serviços podem levar até 11 minutos para parar.

3. Faça logout do shell de comando: `exit`

Informações relacionadas

[Forçar o serviço a terminar](#)

Coloque o aparelho no modo de manutenção

Deve colocar o aparelho no modo de manutenção antes de efetuar procedimentos de manutenção específicos.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Manutenção ou Acesso root. Para obter detalhes, consulte as instruções para administrar o StorageGRID.

Sobre esta tarefa

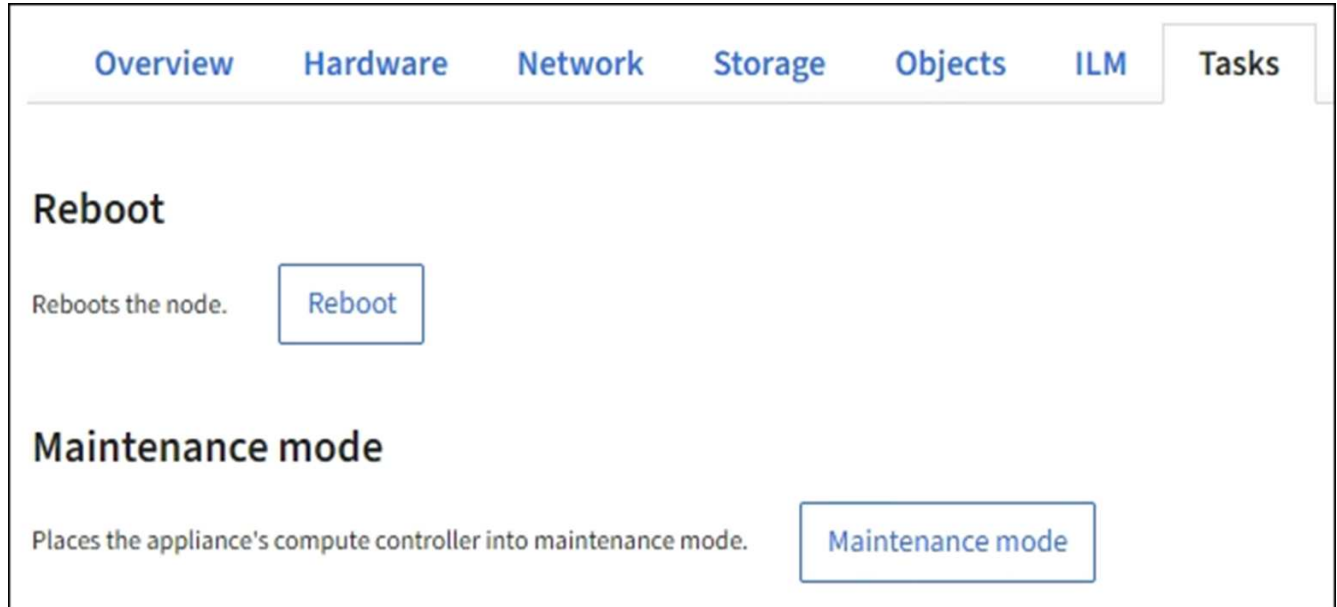
Em casos raros, colocar um dispositivo StorageGRID no modo de manutenção pode tornar o dispositivo indisponível para acesso remoto.



A senha da conta de administrador e as chaves de host SSH para um dispositivo StorageGRID no modo de manutenção permanecem as mesmas que eram quando o dispositivo estava em serviço.

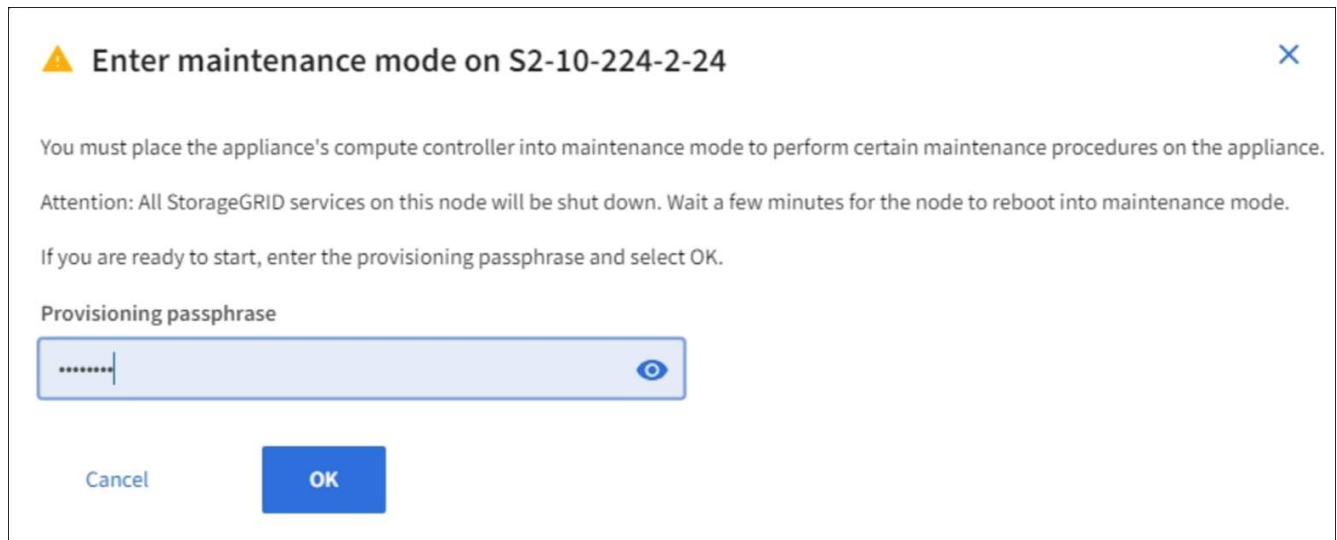
Passos

1. No Gerenciador de Grade, selecione **NÓS**.
2. Na exibição em árvore da página nós, selecione o nó de storage do dispositivo.
3. Selecione **tarefas**.



4. Selecione **modo de manutenção**.

É apresentada uma caixa de diálogo de confirmação.



5. Introduza a frase-passe de provisionamento e selecione **OK**.

Uma barra de progresso e uma série de mensagens, incluindo "Request Sent" (pedido enviado), "Stop StorageGRID" (Paragem) e "Reboot" (reinício), indicam que o aparelho está a concluir os passos para entrar no modo de manutenção.

S2-10-224-2-24 (Storage Node) [↗](#) ✕

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)


Reboot

Reboots the node. [Reboot](#)

Maintenance mode

Places the appliance's compute controller into maintenance mode. [Maintenance mode](#)

⚠ Attention
Your request has been sent, but the appliance might take 10-15 minutes to enter maintenance mode. **Do not perform maintenance procedures until this tab indicates maintenance mode is ready, or data could become corrupted.**

 Rebooting...

Quando o dispositivo está no modo de manutenção, uma mensagem de confirmação lista os URLs que você pode usar para acessar o Instalador do StorageGRID Appliance.

S2-10-224-2-24 (Storage Node) [↗](#) ✕

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)

Reboot

Reboots the node. [Reboot](#)

Maintenance mode

Places the appliance's compute controller into maintenance mode. [Maintenance mode](#)

i This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.24:8443>
- <https://10.224.2.24:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by selecting Reboot Controller from the StorageGRID Appliance Installer.

6. Para acessar o Instalador do StorageGRID Appliance, navegue até qualquer um dos URLs exibidos.
Se possível, use o URL que contém o endereço IP da porta Admin Network do dispositivo.



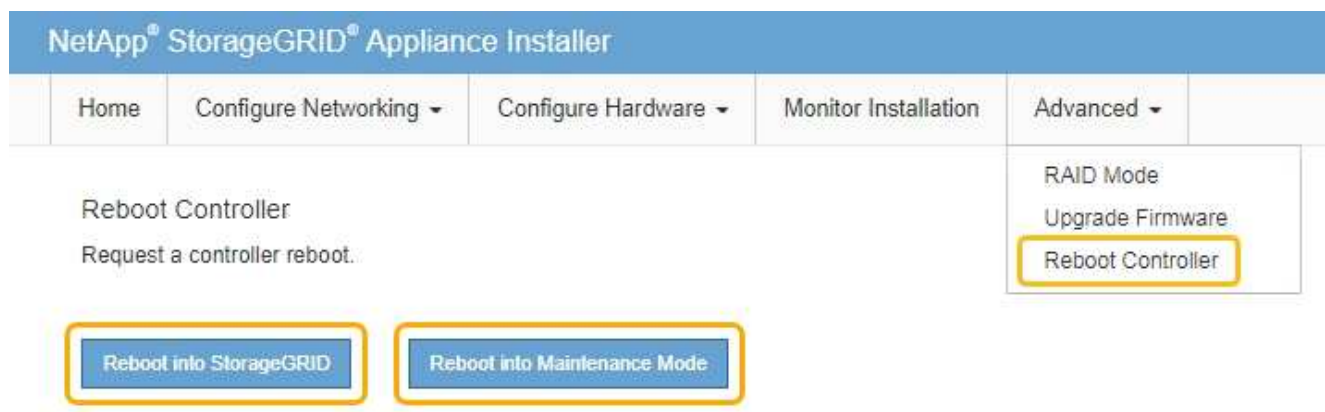
O acesso `https://169.254.0.1:8443` requer uma conexão direta com a porta de gerenciamento local.

7. A partir do instalador do dispositivo StorageGRID, confirme se o aparelho está no modo de manutenção.

This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

8. Execute todas as tarefas de manutenção necessárias.

9. Depois de concluir as tarefas de manutenção, saia do modo de manutenção e retome a operação normal do nó. No Instalador de dispositivos StorageGRID, selecione **Avançado controlador de reinicialização** e, em seguida, selecione **Reiniciar no StorageGRID**.



Pode demorar até 20 minutos para o aparelho reiniciar e voltar a ligar a grelha. Para confirmar que a reinicialização está concluída e que o nó voltou a ingressar na grade, volte ao Gerenciador de Grade. A página **nós** deve exibir um status normal (sem ícones à esquerda do nome do nó) para o nó do dispositivo, indicando que não há alertas ativos e o nó está conectado à grade.

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 14

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	—	—	5%
DC1-ARC1	Archive Node	—	—	2%
DC1-G1	Gateway Node	—	—	2%
DC1-S1	Storage Node	0%	0%	12%
DC1-S2	Storage Node	0%	0%	11%
DC1-S3	Storage Node	0%	0%	11%

Forçar o serviço a terminar

Se você precisar parar um serviço imediatamente, você pode usar o `force-stop` comando.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Forçar manualmente o serviço a terminar: `service servicename force-stop`

Por exemplo:

```
service ldr force-stop
```

O sistema aguarda 30 segundos antes de terminar o serviço.

3. Faça logout do shell de comando: `exit`

Inicie ou reinicie o serviço

Talvez seja necessário iniciar um serviço que tenha sido interrompido ou talvez seja necessário parar e reiniciar um serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

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

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

2. Decida qual comando emitir, com base se o serviço está em execução ou parado no momento.

- Se o serviço estiver parado no momento, use o `start` comando para iniciar o serviço manualmente:
`service servicename start`

Por exemplo:

```
service ldr start
```

- Se o serviço estiver atualmente em execução, use o `restart` comando para parar o serviço e, em seguida, reinicie-o: `service servicename restart`

Por exemplo:

```
service ldr restart
```

+



Utilizar o `restart` comando é o mesmo que utilizar o `stop` comando seguido do `start` comando. Você pode emitir `restart` mesmo se o serviço estiver parado no momento.

3. Faça logout do shell de comando: `exit`

Remova os remapas de portas

Se você quiser configurar um ponto de extremidade para o serviço Load Balancer e quiser usar uma porta que já tenha sido configurada como a porta mapeada de um remapeamento de porta, primeiro remova o remapeamento de porta existente ou o ponto de extremidade não será efetivo. É necessário executar um script em cada nó Admin e nó Gateway que tenha portas remapeadas conflitantes para remover todos os remapeados de portas do nó.



Sobre esta tarefa

Este procedimento remove todos os remapas de portas. Se você precisar manter alguns dos remapas, entre em Contato com o suporte técnico.

Para obter informações sobre como configurar pontos de extremidade do balanceador de carga, consulte as instruções para administrar o StorageGRID.



Se o remapeamento de portas fornecer acesso ao cliente, o cliente deve ser reconfigurado para usar uma porta diferente configurada como um endpoint de balanceador de carga, se possível, para evitar a perda de serviço, caso contrário, remover o mapeamento de portas resultará na perda de acesso ao cliente e deve ser programado adequadamente.



Este procedimento não funciona para um sistema StorageGRID implantado como um contentor em hosts de metal nu. Consulte as instruções para [remoção de remapas de portas em hosts bare metal](#).

Passos

1. Faça login no nó.
 - a. Introduza o seguinte comando: `ssh -p 8022 admin@node_IP`

A porta 8022 é a porta SSH do sistema operacional base, enquanto a porta 22 é a porta SSH do mecanismo de contentor que executa o StorageGRID.

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

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

2. Execute o seguinte script: `remove-port-remap.sh`
3. Reinicie o nó.

Siga as instruções para [reiniciando um nó de grade](#).

4. Repita estas etapas em cada nó de administração e nó de gateway que tenha portas remapeadas conflitantes.

Informações relacionadas

[Administrar o StorageGRID](#)

Remova os remapas de portas em hosts bare metal

Se você quiser configurar um ponto de extremidade para o serviço Load Balancer e quiser usar uma porta que já tenha sido configurada como a porta mapeada de um remapeamento de porta, primeiro remova o remapeamento de porta existente ou o ponto de extremidade não será efetivo. Se você estiver executando o StorageGRID em hosts bare metal, siga este procedimento em vez do procedimento geral para remover os remapas de portas. Você deve editar o arquivo de configuração de nó para cada nó Admin e nó Gateway que tenha portas remapeadas conflitantes para remover todos os remapas de portas do nó e reiniciar o nó.



Sobre esta tarefa

Este procedimento remove todos os remapas de portas. Se você precisar manter alguns dos remapas, entre em Contato com o suporte técnico.

Para obter informações sobre como configurar pontos de extremidade do balanceador de carga, consulte as instruções para administrar o StorageGRID.



Este procedimento pode resultar em perda temporária de serviço à medida que os nós são reiniciados.

Passos

1. Faça login no host que suporta o nó. Faça login como root ou com uma conta que tenha permissão sudo.
2. Execute o seguinte comando para desativar temporariamente o nó: `sudo storagegrid node stop node-name`
3. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó para o nó.

O arquivo de configuração do nó pode ser encontrado em `/etc/storagegrid/nodes/node-name.conf`.

4. Localize a seção do arquivo de configuração do nó que contém os remapas de portas.

Veja as duas últimas linhas no exemplo a seguir.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Edite as entradas `port_REMAP` e `port_REMAP_INBOUND` para remover os remaps de portas.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó para o nó:
`sudo storagegrid node validate node-name`

Solucione quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

7. Execute o seguinte comando para reiniciar o nó sem remaps de portas: `sudo storagegrid node start node-name`
8. Faça login no nó como administrador usando a senha listada no `Passwords.txt` arquivo.
9. Verifique se os serviços começam corretamente.
 - a. Veja uma lista dos status de todos os serviços no servidor: `sudo storagegrid-status`

O estado é atualizado automaticamente.

b. Aguarde até que todos os serviços tenham um status de execução ou verificado.

c. Saia do ecrã de estado:Ctrl+C

10. Repita estas etapas em cada nó de administração e nó de gateway que tenha portas remapeadas conflitantes.

Reinicie o nó da grade

Você pode reinicializar um nó de grade a partir do Gerenciador de Grade ou do shell de comando do nó.

Sobre esta tarefa

Quando você reinicializa um nó de grade, o nó desliga e reinicia. Todos os serviços são reiniciados automaticamente.

Se você planeja reinicializar os nós de storage, observe o seguinte:

- Se uma regra ILM especificar um comportamento de ingestão de confirmação dupla ou a regra especificar balanceado e não for possível criar imediatamente todas as cópias necessárias, o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo local e avaliará o ILM posteriormente. Se você quiser reinicializar dois ou mais nós de storage em um determinado site, talvez não seja possível acessar esses objetos durante a reinicialização.
- Para garantir que você possa acessar todos os objetos enquanto um nó de armazenamento estiver reiniciando, pare de ingerir objetos em um site por aproximadamente uma hora antes de reiniciar o nó.

Informações relacionadas

[Administrar o StorageGRID](#)

Reinicie o nó da grade do Gerenciador de Grade

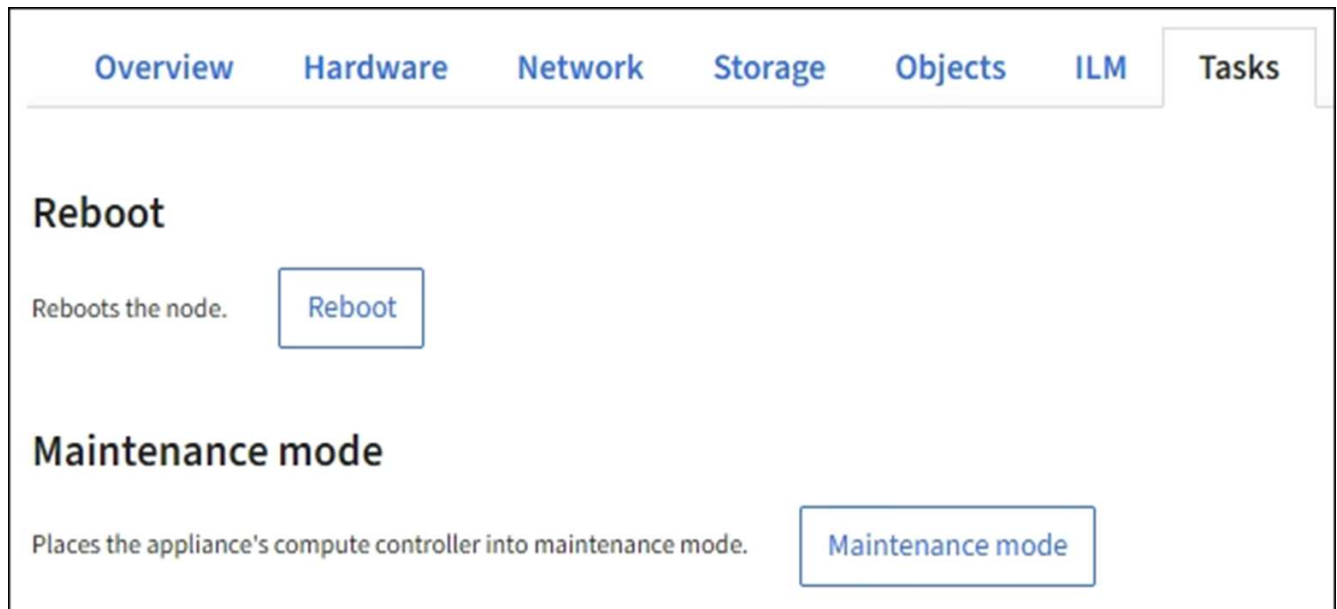
Reiniciar um nó de grade a partir do Gerenciador de Grade emite o `reboot` comando no nó de destino.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento.

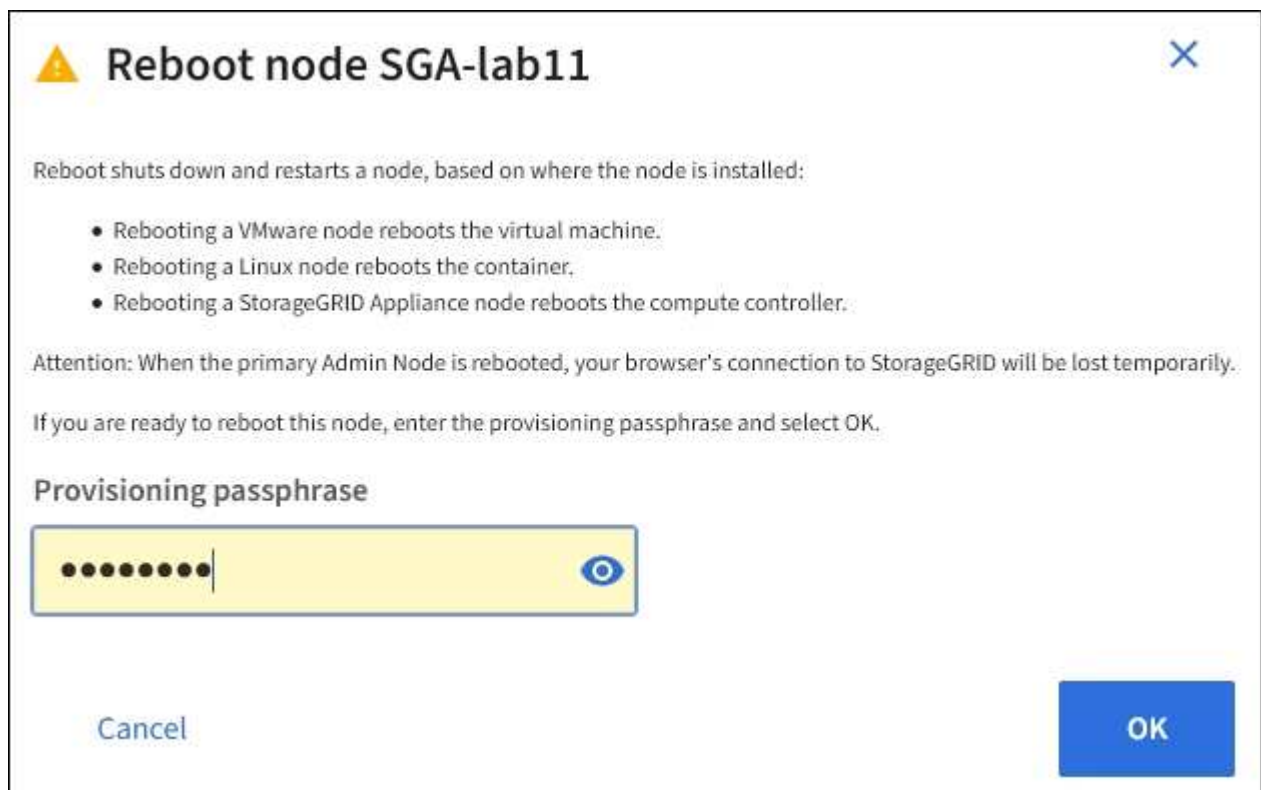
Passos

1. Selecione **NODES**.
2. Selecione o nó de grade que deseja reinicializar.
3. Selecione a guia **tarefas**.



4. Selecione **Reboot**.

É apresentada uma caixa de diálogo de confirmação.



Se você estiver reinicializando o nó Admin principal, a caixa de diálogo de confirmação lembra que a conexão do seu navegador com o Gerenciador de Grade será perdida temporariamente quando os serviços forem interrompidos.

5. Digite a senha de provisionamento e clique em **OK**.

6. Aguarde até que o nó seja reiniciado.

Pode levar algum tempo para que os serviços sejam desativados.

Quando o nó é reinicializado, o ícone cinza (administrativamente para baixo) aparece no lado esquerdo da página **nodes**. Quando todos os serviços forem iniciados novamente e o nó for conectado com êxito à grade, a página **nós** deve exibir um status normal (sem ícones à esquerda do nome do nó), indicando que nenhum alerta está ativo e o nó está conectado à grade.

Reinicie o nó de grade a partir do shell de comando

Se você precisar monitorar a operação de reinicialização mais de perto ou se não conseguir acessar o Gerenciador de Grade, você pode fazer login no nó de grade e executar o comando de reinicialização do Gerenciador de servidor a partir do shell de comando.

Tem de ter o `Passwords.txt` ficheiro.

1. Faça login no nó da grade:

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

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

2. Opcionalmente, pare os serviços: `service servermanager stop`

Parar serviços é um passo opcional, mas recomendado. Os serviços podem levar até 15 minutos para serem encerrados, e você pode querer fazer login no sistema remotamente para monitorar o processo de desligamento antes de reiniciar o nó na próxima etapa.

3. Reinicie o nó da grade: `reboot`

4. Faça logout do shell de comando: `exit`

Encerre o nó da grade

Você pode encerrar um nó de grade a partir do shell de comando do nó.

O que você vai precisar

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

Sobre esta tarefa

Antes de executar este procedimento, reveja estas considerações:

- Em geral, você não deve encerrar mais de um nó de cada vez para evitar interrupções.
- Não encerre um nó durante um procedimento de manutenção, a menos que seja explicitamente instruído a fazê-lo pela documentação ou pelo suporte técnico.
- O processo de desligamento é baseado em onde o nó é instalado, como segue:
 - Desligar um nó da VMware desliga a máquina virtual.

- Desligar um nó Linux desliga o contentor.
- Desligar um nó de dispositivo StorageGRID desliga o controlador de computação.
- Se você planeja encerrar mais de um nó de storage em um local, pare de ingerir objetos nesse local por aproximadamente uma hora antes de desligar os nós.

Se qualquer regra de ILM usar a opção de ingestão **confirmação dupla** (ou se uma regra usar a opção **Balanced** e todas as cópias necessárias não puderem ser criadas imediatamente), o StorageGRID enviará imediatamente quaisquer objetos recém-ingeridos a dois nós de armazenamento no mesmo site e avaliará o ILM mais tarde. Se mais de um nó de storage em um local for desligado, talvez você não consiga acessar objetos recém-ingeridos durante o encerramento. As operações de gravação também podem falhar se houver poucos nós de storage disponíveis no local.

Passos

1. Faça login no nó da grade:

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

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

2. Parar todos os serviços: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem encerrados, e você pode querer fazer login no sistema remotamente para monitorar o processo de desligamento.

3. Se o nó estiver sendo executado em uma máquina virtual VMware ou se for um nó de dispositivo, execute o comando `shutdown`: `shutdown -h now`

Execute esta etapa independentemente do resultado do `service servermanager stop` comando.



Depois de emitir o `shutdown -h now` comando em um nó de dispositivo, você deve desligar o dispositivo para reiniciar o nó.

Para o aparelho, este comando desliga o controlador, mas o aparelho ainda está ligado. Você deve concluir o próximo passo.

4. Se você estiver desativando um nó de dispositivo:

- Para o dispositivo de serviços SG100 ou SG1000
 - i. Desligue a alimentação do aparelho.
 - ii. Aguarde até que o LED azul de alimentação se desligue.
- Para o aparelho SG6000
 - i. Aguarde que o LED verde Cache ative na parte de trás dos controladores de armazenamento se desligue.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

- ii. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.
- Para o aparelho SG5700
 - i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.
 - ii. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

Informações relacionadas

[Administrar o StorageGRID](#)

Desligue o host

Antes de desligar um host, você deve interromper os serviços em todos os nós da grade nesse host.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.Quando você estiver conetado como root, o prompt mudará de `$` para `#`.
2. Parar todos os serviços em execução no nó: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem encerrados, e você pode querer fazer login no sistema remotamente para monitorar o processo de desligamento.
3. Repita as etapas 1 e 2 para cada nó no host.
4. Se você tiver um host Linux:
 - a. Faça login no sistema operacional host.
 - b. Pare o nó: `storagegrid node stop`
 - c. Encerre o sistema operacional do host.
5. Se o nó estiver sendo executado em uma máquina virtual VMware ou se for um nó de dispositivo, execute o comando shutdown: `shutdown -h now`

Execute esta etapa independentemente do resultado do `service servermanager stop` comando.



Depois de emitir o `shutdown -h now` comando em um nó de dispositivo, você deve desligar o dispositivo para reiniciar o nó.

Para o aparelho, este comando desliga o controlador, mas o aparelho ainda está ligado. Você deve

concluir o próximo passo.

6. Se você estiver desativando um nó de dispositivo:

- Para o dispositivo de serviços SG100 ou SG1000
 - i. Desligue a alimentação do aparelho.
 - ii. Aguarde até que o LED azul de alimentação se desligue.
- Para o aparelho SG6000
 - i. Aguarde que o LED verde Cache ative na parte de trás dos controladores de armazenamento se desligue.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

- ii. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.

- Para o aparelho SG5700

- i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

- ii. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

7. Faça logout do shell de comando: `exit`

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

Desligue e ligue todos os nós na rede

Talvez seja necessário desligar todo o sistema StorageGRID, por exemplo, se você estiver movendo um data center. Estas etapas fornecem uma visão geral de alto nível da sequência recomendada para executar um desligamento controlado e inicialização.

Quando você desliga todos os nós em um local ou grade, não será possível acessar objetos ingeridos enquanto os nós de storage estiverem offline.

Pare os serviços e encerre os nós da grade

Antes de poder desligar um sistema StorageGRID, você deve parar todos os serviços em execução em cada nó de grade e, em seguida, desligar todas as máquinas virtuais VMware, mecanismos de contêiner e dispositivos StorageGRID.

Sobre esta tarefa

Pare primeiro os serviços nos nós de administração e nos de API Gateway e, em seguida, pare os serviços nos nós de storage.

Essa abordagem permite que você use o nó de administração principal para monitorar o status dos outros nós de grade pelo maior tempo possível.



Se um único host incluir mais de um nó de grade, não encerre o host até que você tenha parado todos os nós nesse host. Se o host incluir o nó Admin principal, encerre esse host por último.



Se necessário, você pode [Migre nós de um host Linux para outro](#) executar a manutenção do host sem afetar a funcionalidade ou a disponibilidade de sua grade.

Passos

1. Impedir que todas as aplicações cliente acessem à grelha.
2. Faça login em cada nó de gateway:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

3. pare todos os serviços em execução no nó: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem encerrados, e você pode querer fazer login no sistema remotamente para monitorar o processo de desligamento.

4. Repita as duas etapas anteriores para interromper os serviços em todos os nós de storage, nós de arquivamento e nós de administração não primários.

Você pode parar os serviços nesses nós em qualquer ordem.



Se você emitir o `service servermanager stop` comando para parar os serviços em um nó de armazenamento de dispositivo, será necessário desligar o dispositivo para reiniciar o nó.

5. Para o nó de administração principal, repita as etapas para [iniciar sessão no nó](#) e [parando todos os serviços no nó](#).
6. Para nós que estão sendo executados em hosts Linux:
 - a. Faça login no sistema operacional host.
 - b. Pare o nó: `storagegrid node stop`
 - c. Encerre o sistema operacional do host.
7. Para nós que estão sendo executados em máquinas virtuais VMware e para nós de storage do dispositivo, execute o comando shutdown: `shutdown -h now`

Execute esta etapa independentemente do resultado do `service servermanager stop` comando.

Para o dispositivo, esse comando desliga o controlador de computação, mas o dispositivo ainda está ligado. Você deve concluir o próximo passo.

8. Se você tiver nós do dispositivo:

- Para o dispositivo de serviços SG100 ou SG1000
 - i. Desligue a alimentação do aparelho.
 - ii. Aguarde até que o LED azul de alimentação se desligue.
- Para o aparelho SG6000
 - i. Aguarde que o LED verde Cache ative na parte de trás dos controladores de armazenamento se desligue.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

- ii. Desligue o aparelho e aguarde até que o LED azul de alimentação se desligue.
- Para o aparelho SG5700
 - i. Aguarde que o LED verde Cache ative na parte de trás do controlador de armazenamento seja desligado.

Este LED fica aceso quando os dados em cache precisam ser gravados nas unidades. Tem de esperar que este LED se desligue antes de desligar a alimentação.

- ii. Desligue a alimentação do aparelho e aguarde que todas as atividades de exibição de LED e de sete segmentos parem.

9. Se necessário, faça logout do shell de comando: `exit`

A grelha StorageGRID foi agora desligada.

Informações relacionadas

[Aparelhos de serviços SG100 e SG1000](#)

[SG6000 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

Inicie os nós de grade

Siga esta sequência para iniciar os nós da grelha após um encerramento completo.



O que você precisa 8217

Se toda a grade tiver sido desligada por mais de 15 dias, entre em Contato com o suporte técnico antes de iniciar qualquer nó de grade. Não tente os procedimentos de recuperação que reconstruam dados do Cassandra. Isso pode resultar em perda de dados.

Sobre esta tarefa

Se possível, você deve ligar os nós da grade nesta ordem:

- Aplique o poder aos nós de administração primeiro.
- Aplique energia aos nós do Gateway por último.



Se um host incluir vários nós de grade, os nós retornarão online automaticamente quando você ligar o host.

Passos

1. Ligue os hosts para o nó de administração principal e quaisquer nós de administração não primários.



Você não poderá fazer login nos nós de administração até que os nós de storage tenham sido reiniciados.

2. Ligue os hosts para todos os nós de arquivamento e nós de storage.

Você pode ativar esses nós em qualquer ordem.

3. Ligue os hosts para todos os nós do Gateway.
4. Faça login no Gerenciador de Grade.
5. Selecione **NÓS** e monitore o status dos nós da grade. Verifique se não há ícones de alerta ao lado dos nomes dos nós.

The screenshot shows a web interface titled 'Nodes' with a search bar and a table of nodes. The table has columns for Name, Type, Object data used, Object metadata used, and CPU usage. The nodes listed are StorageGRID Deployment, Data Center 1, and several individual nodes (DC1-ADM1, DC1-ARC1, DC1-G1, DC1-S1, DC1-S2, DC1-S3) with their respective types and usage percentages.

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	—	—	5%
DC1-ARC1	Archive Node	—	—	2%
DC1-G1	Gateway Node	—	—	2%
DC1-S1	Storage Node	0%	0%	12%
DC1-S2	Storage Node	0%	0%	11%
DC1-S3	Storage Node	0%	0%	11%

Use um arquivo DoNotStart

Se você estiver executando vários procedimentos de manutenção ou configuração sob a direção do suporte técnico, você pode ser solicitado a usar um arquivo DoNotStart para impedir que os serviços iniciem quando o Gerenciador de servidor é iniciado ou reiniciado.



Você deve adicionar ou remover um arquivo DoNotStart somente se o suporte técnico o tiver direcionado para fazê-lo.

Para impedir que um serviço seja iniciado, coloque um arquivo DoNotStart no diretório do serviço que você deseja impedir de iniciar. No arranque, o Gestor de servidor procura o ficheiro DoNotStart. Se o arquivo estiver presente, o serviço (e quaisquer serviços que dependem dele) é impedido de iniciar. Quando o arquivo DoNotStart é removido, o serviço interrompido anteriormente será iniciado no próximo início ou reinício do Server Manager. Os serviços não são iniciados automaticamente quando o arquivo DoNotStart é removido.

A maneira mais eficiente de impedir que todos os serviços sejam reiniciados é impedir que o serviço NTP seja iniciado. Todos os serviços dependem do serviço NTP e não podem ser executados se o serviço NTP não estiver em execução.

Adicione o arquivo DoNotStart para o serviço

Você pode impedir que um serviço individual comece adicionando um arquivo DoNotStart ao diretório desse serviço em um nó de grade.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:

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

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

2. Adicione um arquivo DoNotStart: `touch /etc/sv/service/DoNotStart`

```
`service` onde está o nome do serviço a ser impedido de iniciar. Por exemplo,
```

```
touch /etc/sv/ldr/DoNotStart
```

É criado um ficheiro DoNotStart. Nenhum conteúdo de arquivo é necessário.

Quando o Gerenciador de servidor ou o nó de grade é reiniciado, o Gerenciador de servidor será reiniciado, mas o serviço não será reiniciado.

3. Faça logout do shell de comando: `exit`

Remova o arquivo DoNotStart para serviço

Quando você remove um arquivo DoNotStart que está impedindo que um serviço seja iniciado, você deve iniciar esse serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Remova o arquivo DoNotStart do diretório de serviços: `rm /etc/sv/service/DoNotStart`

```
`service`onde está o nome do serviço. Por exemplo,
```

```
rm /etc/sv/ldr/DoNotStart
```

3. Inicie o serviço: `service servicename start`
4. Faça logout do shell de comando: `exit`

Solucionar problemas do Server Manager

Accesse o arquivo de log do Server Manager

Se surgir um problema ao utilizar o Gestor de servidor, verifique o respetivo ficheiro de registo.

As mensagens de erro relacionadas ao Gestor de servidor são capturadas no ficheiro de registo do Gestor de servidor, que se encontra em: `/var/local/log/servermanager.log`

Verifique este arquivo para ver se há mensagens de erro relacionadas a falhas. Encaminhe o problema para o suporte técnico, se necessário. Poderá ser-lhe pedido que encaminhe ficheiros de registo para o suporte técnico.

Serviço com um estado de erro

Se detetar que um serviço introduziu um estado de erro, tente reiniciar o serviço.

O que você vai precisar

Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

O Server Manager monitora os serviços e reinicia qualquer um que tenha parado inesperadamente. Se um serviço falhar, o Gerenciador do servidor tentará reiniciá-lo. Se houver três tentativas falhadas de iniciar um serviço dentro de cinco minutos, o serviço entrará em um estado de erro. O Gerenciador de servidores não tenta outra reinicialização.

Passos

1. Faça login no nó da grade:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

2. Confirme o estado de erro do serviço: `service servicename status`

Por exemplo:

```
service ldr status
```

Se o serviço estiver em um estado de erro, a seguinte mensagem será retornada: `servicename in error state`. Por exemplo:

```
ldr in error state
```



Se o status do serviço for `disabled`, consulte as instruções para [Removendo um arquivo DoNotStart para um serviço](#).

3. Tente remover o estado de erro reiniciando o serviço: `service servicename restart`

Se o serviço não reiniciar, contacte o suporte técnico.

4. Faça logout do shell de comando: `exit`

Clonagem do nó do dispositivo

Você pode clonar um nó de dispositivo no StorageGRID para usar um dispositivo de design mais recente ou recursos aprimorados. A clonagem transfere todas as informações do nó existente para o novo dispositivo, fornece um processo de atualização de hardware fácil de executar e fornece uma alternativa à desativação e expansão para a substituição de dispositivos.

Como funciona a clonagem de nós do dispositivo

A clonagem do nó do dispositivo permite substituir facilmente um nó do dispositivo (origem) existente na grade por um dispositivo compatível (destino) que faz parte do mesmo local lógico da StorageGRID. O processo transfere todos os dados para o novo dispositivo, colocando-os em serviço para substituir o nó antigo do dispositivo e deixando o dispositivo antigo em um estado de pré-instalação.

Por que clonar um nó de dispositivo?

Você pode clonar um nó de dispositivo se precisar:

- Substitua os aparelhos que estão chegando ao fim da vida útil.
- Atualize os nós existentes para aproveitar a tecnologia aprimorada do dispositivo.
- Aumente a capacidade de storage em grade sem alterar o número de nós de storage no sistema StorageGRID.
- Aumentar a eficiência de storage, como alterar o modo RAID de DDP-8 para DDP-16 ou RAID-6.
- Implemente com eficiência a criptografia de nó para permitir o uso de servidores de gerenciamento de chaves externas (KMS).

Que rede StorageGRID é utilizada?

A clonagem transfere dados do nó de origem diretamente para o dispositivo de destino em qualquer uma das três redes StorageGRID. Normalmente, a rede de Grade é utilizada, mas também pode utilizar a rede Admin ou a rede Cliente se o utilitário de origem estiver ligado a estas redes. Escolha a rede a ser usada para clonagem de tráfego que forneça a melhor performance de transferência de dados sem prejudicar a performance da rede StorageGRID ou a disponibilidade de dados.

Ao instalar o dispositivo de substituição, você deve especificar endereços IP temporários para conexão StorageGRID e transferência de dados. Como o dispositivo de substituição fará parte das mesmas redes que o nó do dispositivo que ele substitui, você deve especificar endereços IP temporários para cada uma dessas redes no dispositivo de substituição.

Compatibilidade do dispositivo alvo

Os dispositivos de substituição devem ser do mesmo tipo que o nó de origem que estão substituindo e ambos devem fazer parte do mesmo local lógico do StorageGRID.

- Um dispositivo de serviços de substituição pode ser diferente do nó de administração ou do nó de gateway que está substituindo.
 - Você pode clonar um dispositivo de nó de origem SG100 para um dispositivo de destino de serviços SG1000 para oferecer maior capacidade ao nó de administrador ou nó de gateway.
 - Você pode clonar um dispositivo de nós de origem SG1000 para um dispositivo de destino de serviços SG100 para replantar o SG1000 para uma aplicação mais exigente.

Por exemplo, se um dispositivo de nó de origem SG1000 estiver sendo usado como nó Admin e você quiser usá-lo como um nó de balanceamento de carga dedicado.

- A substituição de um dispositivo de nó de origem SG1000 por um dispositivo de destino de serviços SG100 reduz a velocidade máxima das portas de rede de 100 GbE para 25 GbE.
- Os aparelhos SG100 e SG1000 têm conetores de rede diferentes. Mudar o tipo de aparelho pode

exigir a substituição dos cabos ou módulos SFP.

- Um dispositivo de storage de substituição deve ter capacidade igual ou superior ao nó de storage que está substituindo.
 - Se o dispositivo de armazenamento de destino tiver o mesmo número de unidades que o nó de origem, as unidades no dispositivo de destino devem ter maior capacidade (em TB).
 - Se você planeja usar o mesmo modo RAID no nó de destino que foi usado no nó de origem ou um modo RAID com menos eficiência de armazenamento (por exemplo, alternar de RAID6 para DDP), as unidades no dispositivo de destino devem ser maiores (em TB) do que as unidades no dispositivo de origem.
 - Se o número de unidades padrão instaladas em um dispositivo de armazenamento de destino for menor que o número de unidades no nó de origem, devido à instalação de unidades de estado sólido (SSDs), a capacidade geral de armazenamento das unidades padrão no dispositivo de destino (em TB) deve atender ou exceder a capacidade total da unidade funcional de todas as unidades no nó de armazenamento de origem.

Por exemplo, ao clonar um dispositivo de nó de storage de SG5660 fontes com 60 unidades para um dispositivo de destino de SG6060 TB ou SG6060X TB com 58 unidades padrão, unidades maiores devem ser instaladas no dispositivo de destino de SG6060 TB ou SG6060X TB antes da clonagem para manter a capacidade de storage. (Os dois slots de unidade que contêm SSDs no dispositivo de destino não estão incluídos na capacidade total de armazenamento do dispositivo.)

No entanto, se um dispositivo de nó de origem de SG5660 unidades de 60 16 U estiver configurado com DDP-8 SANtricity Dynamic Disk Pools, configurar um dispositivo de destino de SG6060 ou SG6060X unidades com DDP-58 pode tornar o dispositivo SG6060 ou SG6060X um destino válido devido à sua eficiência de storage aprimorada.

Você pode exibir informações sobre o modo RAID atual do nó do dispositivo de origem na página **NÓS** no Gerenciador de Grade. Selecione o separador **Storage** (armazenamento) para o aparelho.

Que informação não é clonada?

As configurações do dispositivo a seguir não são transferidas para o dispositivo de substituição durante a clonagem. Deve configurá-los durante a configuração inicial do aparelho de substituição.

- Interface BMC
- Ligações de rede
- Status da criptografia do nó
- Gerenciador de sistema do SANtricity (para nós de storage)
- Modo RAID (para nós de storage)

Que problemas impedem a clonagem?

Se algum dos seguintes problemas for encontrado durante a clonagem, o processo de clonagem será interrompido e uma mensagem de erro será gerada:

- Configuração de rede incorreta
- Falta de conectividade entre os dispositivos de origem e destino
- Incompatibilidade de dispositivos de origem e destino
- Para nós de storage, um dispositivo de substituição de capacidade insuficiente

Para continuar, é necessário resolver cada problema de clonagem.

Considerações e requisitos para clonagem de nós do dispositivo

Antes de clonar um nó do dispositivo, você precisa entender as considerações e os requisitos.

Requisitos de hardware para o dispositivo de substituição

Certifique-se de que o aparelho de substituição cumpre os seguintes critérios:

- O nó de origem (dispositivo sendo substituído) e o dispositivo de destino (novo) devem ser do mesmo tipo de dispositivo:
 - Você só pode clonar um dispositivo Admin Node ou um dispositivo Gateway Node para um novo dispositivo de serviços.
 - Você só pode clonar um dispositivo nó de storage para um novo dispositivo de storage.
- Para os dispositivos Admin Node ou Gateway Node, o dispositivo de nó de origem e o dispositivo de destino não precisam ser do mesmo tipo de dispositivo; no entanto, alterar o tipo de dispositivo pode exigir a substituição dos cabos ou módulos SFP.

Por exemplo, você pode substituir um dispositivo de SG1000 nós por um SG100 ou substituir um dispositivo SG100 por um dispositivo SG1000.

- Para dispositivos Storage Node, o dispositivo de nó de origem e o dispositivo de destino não precisam ser do mesmo tipo de dispositivo. No entanto, o dispositivo de destino deve ter maior capacidade de storage do que o dispositivo de origem.

Por exemplo, você pode substituir um dispositivo de SG5600 nós por um dispositivo SG5700 ou SG6000.

Entre em Contato com seu representante de vendas da StorageGRID para obter ajuda na escolha de dispositivos de substituição compatíveis para clonar nós de dispositivos específicos em sua instalação do StorageGRID.

Prepare-se para clonar um nó de dispositivo

Você precisa ter as seguintes informações antes de clonar um nó de dispositivo:

- Obtenha um endereço IP temporário para a rede de Grade do administrador da rede para uso com o utilitário de destino durante a instalação inicial. Se o nó de origem pertencer a uma rede de administração ou a uma rede de cliente, obtenha endereços IP temporários para essas redes.

Os endereços IP temporários estão normalmente na mesma sub-rede que o dispositivo de nó de origem que está sendo clonado e não são necessários após a conclusão da clonagem. Os dispositivos de origem e destino devem se conectar ao nó de administrador principal do StorageGRID para estabelecer uma conexão de clonagem.

- Determinar qual rede usar para clonar o tráfego de transferência de dados que forneça a melhor performance de transferência de dados sem prejudicar a performance da rede StorageGRID ou a disponibilidade de dados.



O uso da rede de administração de 1 GbE para clonar a transferência de dados resulta em clonagem mais lenta.

- Determine se a criptografia de nó usando um servidor de gerenciamento de chaves (KMS) será usada no dispositivo de destino, de modo que você possa habilitar a criptografia de nó durante a instalação inicial do dispositivo de destino antes da clonagem. Você pode verificar se a criptografia de nó está ativada no nó do dispositivo de origem, conforme descrito na instalação do dispositivo.

O nó de origem e o dispositivo de destino podem ter configurações diferentes de criptografia de nó. A descriptografia e a criptografia de dados são executadas automaticamente durante a transferência de dados e quando o nó de destino é reiniciado e se junta à grade.

- [Aparelhos de serviços SG100 e SG1000](#)
- [SG5600 dispositivos de armazenamento](#)
- [SG5700 dispositivos de armazenamento](#)
- [SG6000 dispositivos de armazenamento](#)

- Determine se o modo RAID no dispositivo de destino deve ser alterado de sua configuração padrão, para que você possa especificar essas informações durante a instalação inicial do dispositivo de destino antes da clonagem. Você pode exibir informações sobre o modo RAID atual do nó do dispositivo de origem na página **NÓS** no Gerenciador de Grade. Selecione o separador **Storage** (armazenamento) para o aparelho.

O nó de origem e o dispositivo de destino podem ter configurações RAID diferentes.

- Planeje por tempo suficiente para concluir o processo de clonagem de nós. Vários dias podem ser necessários para transferir dados de um nó de armazenamento operacional para um dispositivo de destino. Agende a clonagem em um momento que minimize o impacto nos negócios.
- Você só deve clonar um nó de dispositivo de cada vez. A clonagem pode impedir que você execute outras funções de manutenção do StorageGRID ao mesmo tempo.
- Depois de clonar um nó de dispositivo, você pode usar o dispositivo de origem que foi retornado a um estado de pré-instalação como destino para clonar outro dispositivo de nó compatível.

Nó do dispositivo clone

O processo de clonagem pode levar vários dias para transferir dados entre o nó de origem (o dispositivo está sendo substituído) e o dispositivo de destino (novo).

O que você vai precisar

- Você instalou o dispositivo de destino compatível em um gabinete ou rack, conectou todos os cabos e aplicou energia.
- Você verificou que a versão do Instalador de dispositivos StorageGRID no dispositivo de substituição corresponde à versão de software do seu sistema StorageGRID, atualizando o firmware do Instalador de dispositivos StorageGRID, se necessário.
- Você configurou o dispositivo de destino, incluindo a configuração de conexões StorageGRID, o Gerenciador de sistema do SANtricity (somente dispositivos de storage) e a interface do BMC.
 - Ao configurar conexões StorageGRID, use os endereços IP temporários.
 - Ao configurar links de rede, use a configuração final do link.



Deixe o Instalador do StorageGRID Appliance aberto depois de concluir a configuração inicial do dispositivo de destino. Você retornará à página do instalador do dispositivo de destino depois de iniciar o processo de clonagem do nó.

- Você ativou opcionalmente a criptografia de nó para o dispositivo de destino.

- Opcionalmente, você definiu o modo RAID para o dispositivo de destino (somente dispositivos de armazenamento).
- [Considerações e requisitos para clonagem de nós do dispositivo](#)

[Aparelhos de serviços SG100 e SG1000](#)

[SG5600 dispositivos de armazenamento](#)

[SG5700 dispositivos de armazenamento](#)

[SG6000 dispositivos de armazenamento](#)

Você deve clonar apenas um nó do dispositivo de cada vez para manter o desempenho da rede StorageGRID e a disponibilidade de dados.

Passos

1. [Coloque o nó de origem que você está clonando no modo de manutenção.](#)
2. No Instalador de dispositivos StorageGRID no nó de origem, na seção Instalação da página inicial, selecione **Ativar clonagem**.

NetApp® StorageGRID® Appliance Installer Help

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

This Node

Node type: Storage ▾

Node name: hrmny2-1-254-sn

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery:

Primary Admin Node IP: 172.16.0.62

Connection state: Connection to 172.16.0.62 ready.

Cancel Save

Installation

Current state: Maintenance mode. [Reboot](#) the node to resume normal operation.

Start Expansion **Enable Cloning**

A seção de conexão do nó de administração principal é substituída pela seção de conexão do nó de destino Clone.

NetApp® StorageGRID® Appliance Installer Help

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

This Node

Node type: Storage ▾

Node name: hrmny2-1-254-sn

Cancel
Save

Clone target node connection

Clone target node IP: 0.0.0.0

Connection state: No connection information available.

Cancel
Save

Installation

Current state: Waiting for configuration and validation of clone target.

Start Cloning
Disable Cloning

3. Para **Clone IP do nó de destino**, insira o endereço IP temporário atribuído ao nó de destino para que a rede use para clonar tráfego de transferência de dados e selecione **Salvar**.

Normalmente, você insere o endereço IP da rede de Grade, mas se precisar usar uma rede diferente para clonar tráfego de transferência de dados, insira o endereço IP do nó de destino nessa rede.



O uso da rede de administração de 1 GbE para clonar a transferência de dados resulta em clonagem mais lenta.

Depois que o utilitário de destino é configurado e validado, na seção Instalação, **Iniciar clonagem** é ativado no nó de origem.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

ℹ The cloning process is ready to be started. Select **Start Cloning** when you are ready. To terminate cloning before it completes and return this node to service, trigger a reboot.

This Node

Node type

Storage ▾

Node name

hmnny2-1-254-sn

Cancel

Save

Clone target node connection

Clone target node IP

10.224.1.253

Connection state

Connection to 10.224.1.253 ready.

Cancel

Save

Installation

Current state

Ready to start cloning all data from this node to the clone target node using the Admin Network connection.
 ⚠ Attention: the Admin Network typically has less bandwidth than the Grid or Client Networks. Use the Grid or Client IP of the target node for faster cloning.

Start Cloning

Disable Cloning

Se existirem problemas que impeçam a clonagem, **Iniciar clonagem** não está ativada e os problemas que você deve resolver são listados como **estado de conexão**. Esses problemas são listados na página inicial do instalador do dispositivo StorageGRID do nó de origem e do dispositivo de destino. Apenas um problema é exibido de cada vez e o estado é atualizado automaticamente à medida que as condições mudam. Resolva todos os problemas de clonagem para ativar **Iniciar clonagem**.

Quando **Iniciar clonagem** está ativada, o **estado atual** indica a rede StorageGRID selecionada para o tráfego de clonagem, juntamente com informações sobre como usar essa conexão de rede.

Considerações e requisitos para clonagem de nós do dispositivo

4. Selecione **Iniciar clonagem** no nó de origem.
5. Monitore o progresso da clonagem usando o instalador do StorageGRID Appliance no nó de origem ou de destino.

O Instalador do StorageGRID Appliance nos nós de origem e destino indica o mesmo status.

NetApp® StorageGRID® Appliance Installer Help

Home | Configure Networking ▾ | Configure Hardware ▾ | Monitor Installation | Advanced ▾

Monitor Cloning

1. Establish clone peering relationship		Complete
2. Clone another node from this node		Running
Step	Progress	Status
Send data to clone target node	<div style="width: 10%;"></div>	Sending data, 0% complete, 8.99 GB transferred
3. Activate cloned node and leave this one offline		Pending

A página monitorar clonagem fornece progresso detalhado para cada etapa do processo de clonagem:

- **Estabelecer relação de peering de clone** mostra o progresso da configuração e configuração da clonagem.
 - **Clone outro nó deste nó** mostra o progresso da transferência de dados. (Esta parte do processo de clonagem pode levar vários dias para ser concluída.)
 - **Ativar nó clonado e deixar este offline** mostra o progresso da transferência de controle para o nó de destino e colocar o nó de origem em um estado de pré-instalação, após a transferência de dados estar concluída.
6. Se você precisar encerrar o processo de clonagem e retornar o nó de origem ao serviço antes de a clonagem ser concluída, no nó de origem vá para a página inicial do Instalador do StorageGRID Appliance e selecione **Avançado > Reiniciar controlador** e, em seguida, selecione **Reiniciar no StorageGRID**.

Se o processo de clonagem for terminado:

- O nó de origem sai do modo de manutenção e regozija-se com o StorageGRID.
- O nó de destino permanece no estado de pré-instalação. Para reiniciar a clonagem do nó de origem, inicie o processo de clonagem novamente a partir da etapa 1.

Quando a clonagem for concluída com sucesso:

- Os nós de origem e destino trocam endereços IP:
 - O nó de destino agora usa os endereços IP originalmente atribuídos ao nó de origem para redes de Grade, Admin e Cliente.
 - O nó de origem agora usa o endereço IP temporário inicialmente atribuído ao nó de destino.
- O nó de destino sai do modo de manutenção e une o StorageGRID, substituindo o nó de origem.
- O dispositivo de origem está em um estado pré-instalado, como se você tivesse [preparou-o para a reinstalação](#).



Se o dispositivo não se juntar novamente à grade, vá para a página inicial do Instalador de dispositivos StorageGRID para o nó de origem, selecione **Avançado > Reiniciar controlador** e, em seguida, selecione **Reiniciar no modo de manutenção**. Depois que o nó de origem for reinicializado no modo de manutenção, repita o procedimento de clonagem do nó.

Os dados do usuário permanecem no dispositivo de origem como uma opção de recuperação se ocorrer um

problema inesperado com o nó de destino. Depois que o nó de destino se juntou ao StorageGRID com sucesso, os dados do usuário no dispositivo de origem ficam desatualizados e não são mais necessários. Se desejar, peça ao suporte StorageGRID para limpar o dispositivo de origem para destruir esses dados.

Você pode:

- Use o dispositivo de origem como destino para operações de clonagem adicionais: nenhuma configuração adicional é necessária. Este dispositivo já tem o endereço IP temporário atribuído que foi originalmente especificado para o primeiro destino clone.
- Instale e configure o dispositivo de origem como um novo nó de dispositivo.
- Deite fora o aparelho de origem se já não for utilizado com o StorageGRID.

Rever registros de auditoria

Revisar logs de auditoria: Visão geral

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e registros de auditoria do StorageGRID. Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções destinam-se aos administradores responsáveis pela produção de relatórios de atividade e utilização do sistema que exijam a análise das mensagens de auditoria do sistema StorageGRID.

Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó Admin.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, [Configurar mensagens de auditoria e destinos de log](#) consulte .

Informações relacionadas

- [Administrar o StorageGRID](#)

Auditoria de fluxo e retenção de mensagens

Todos os serviços StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para `audit.log` o arquivo.

Auditoria do fluxo de mensagens

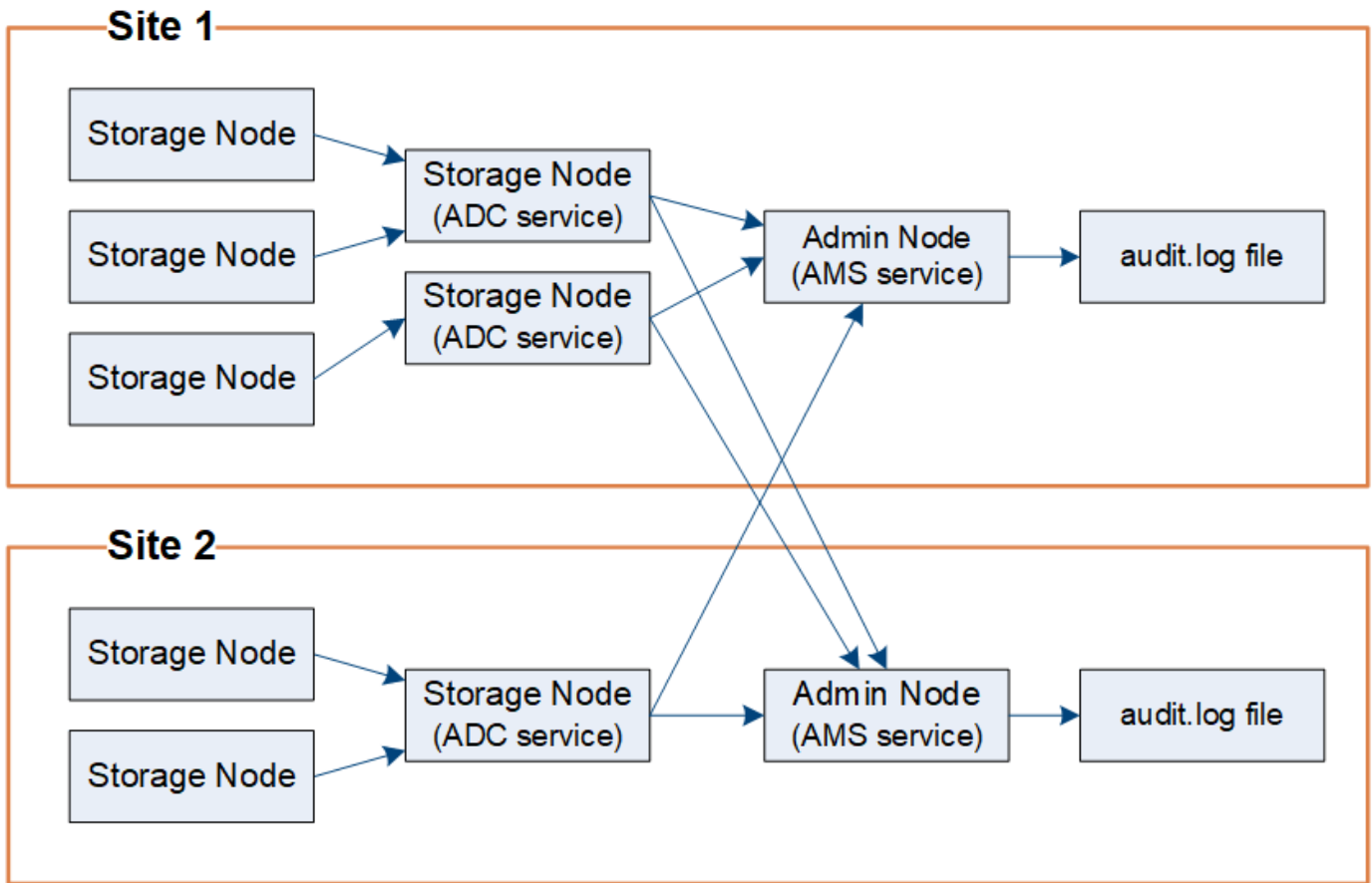
As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços ADC no local do data center. O serviço ADC é ativado automaticamente para os três primeiros nós de storage instalados em cada local.

Por sua vez, cada serviço ADC atua como um relé e envia sua coleção de mensagens de auditoria para cada nó de administração no sistema StorageGRID, o que dá a cada nó de administração um Registro completo da atividade do sistema.

Cada nó Admin armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é

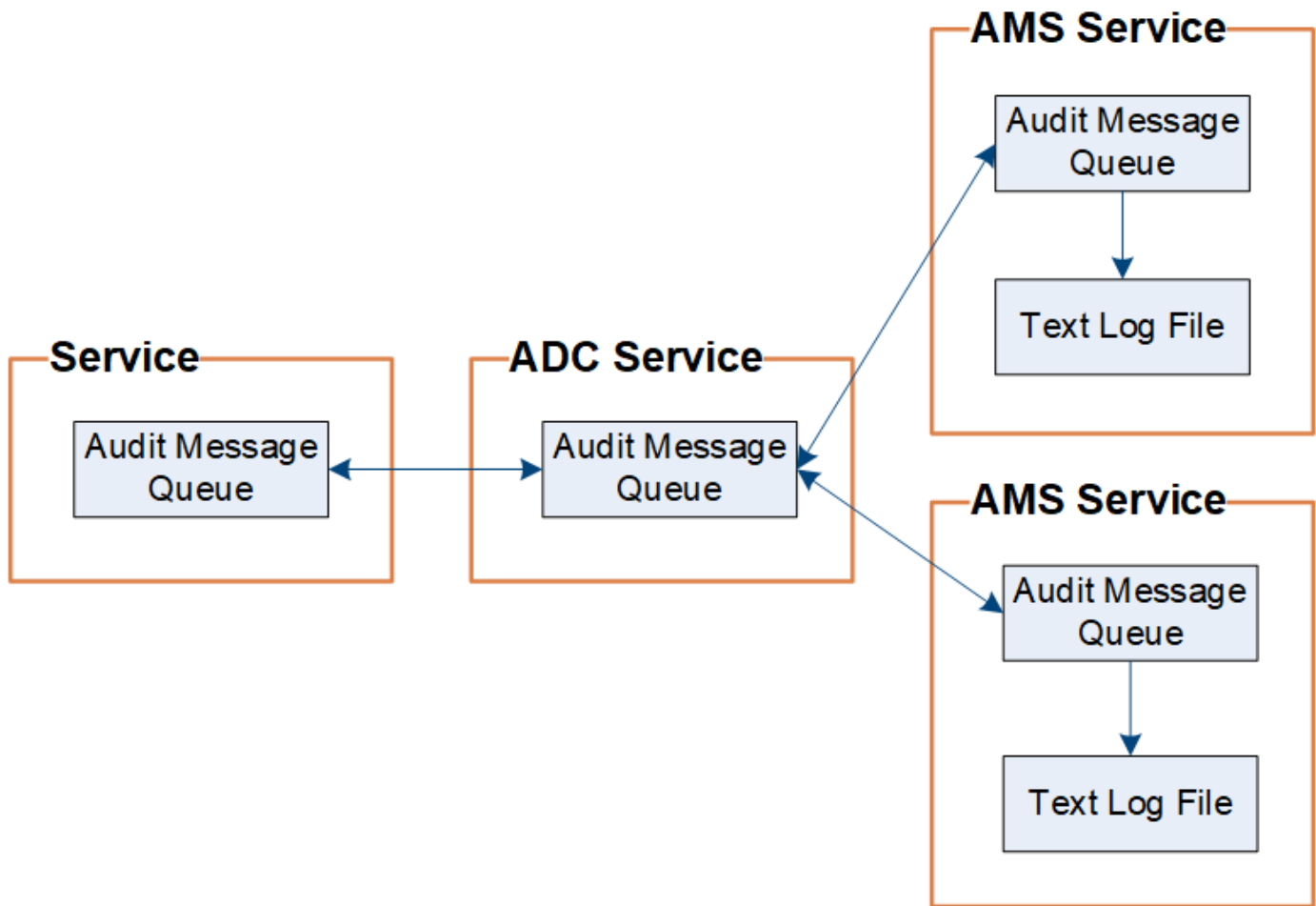
audit.log nomeado .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de cópia e exclusão para garantir que nenhuma mensagem de auditoria seja perdida antes que ela possa ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no diretório do Admin Node `/var/local/audit/export`. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conectividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível no diretório de cada nó `/var/local/`. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/audit/export` diretório usado por um nó Admin ficar cheio, o nó Admin será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações de clientes S3 e Swift não são afetadas. O alarme XAMS (Unreachable Audit Repositories) é acionado quando um repositório de auditoria é inacessível.
- Se o `/var/local/` diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para auditar mensagens até que o diretório esteja apenas 87% cheio. As solicitações de clientes S3 e Swift para outros nós não são afetadas. O alarme NRLY (relés de auditoria disponíveis) é acionado quando os relés de auditoria não são alcançáveis.



Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente `/var/local/log/localaudit.log` no arquivo.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 e Swift com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito grandes:

- A interrupção de um nó de administração ou de um nó de storage com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar com backlogged.
- Uma taxa de atividade contínua que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC se torna cheio por razões não relacionadas às mensagens de auditoria. Quando isso acontece, o nó pára de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria enfileiradas (AMQS)

Para ajudá-lo a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administrador atinge determinados limites.

Se o alerta **fila de auditoria grande** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema - se houver um número significativo de transações recentes, o alerta e o alarme devem ser resolvidos com o tempo e podem ser ignorados.

Se o alerta ou o alarme persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado. Consulte "[Configurar mensagens de auditoria e destinos de log.](#)"

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora se ocorrer uma falha de rede ou nó. Por esse motivo, mensagens duplicadas podem existir no log de auditoria.

Acessar o arquivo de log de auditoria

O compartilhamento de auditoria contém o arquivo ativo `audit.log` e todos os arquivos de log de auditoria compactados. Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente para compartilhamentos de auditoria para NFS e CIFS (CIFS está obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Passos

1. Faça login em um nó Admin:
 - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/audit/export
```

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Informações relacionadas

[Administrar o StorageGRID](#)

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos no diretório de um nó de administrador `/var/local/audit/export`. Os arquivos de log de auditoria ativos são `audit.log` nomeados .



Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos Registros de auditoria continuam a ser gerados e armazenados quando um servidor syslog externo é configurado. [Configurar mensagens de auditoria e destinos de log](#) Consulte .

Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`. Se mais de um log de auditoria for criado em um único dia, os nomes de arquivo usarão a data em que o arquivo foi salvo, anexado por um número, no formato `yyyy-mm-dd.txt.n`. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são os primeiros e segundos arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original. Com o tempo, isso resulta no consumo de storage alocado para logs de auditoria no nó Admin. Um script monitora o consumo de espaço do log de auditoria e exclui arquivos de log conforme necessário para liberar espaço no `/var/local/audit/export` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log`.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Faça auditoria de arquivos de log e formatos de mensagens

Você pode usar logs de auditoria para coletar informações sobre o seu sistema e solucionar problemas. Você deve entender o formato do arquivo de log de auditoria e o formato geral usado para mensagens de auditoria.

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó Admin e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O tempo Universal coordenado (UTC) do evento que acionou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* estão microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT`.

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para legibilidade). Essas mensagens foram geradas quando um locatário criou um bucket do S3 e adicionou dois objetos a esse bucket.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[AVER(UI32):10][ATIM(UI64):1565203410247711]  
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[S3KY(CSTR):"fh-small-0"]  
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-EB44FB4FCC7F"]  
[CSIZ(UI64):1024][AVER(UI32):10]  
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[S3KY(CSTR):"fh-small-2000"]  
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-E578D66F7ADD"]  
[CSIZ(UI64):1024][AVER(UI32):10]  
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

Em seu formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou interpretar. Você pode usar a `audit-explain` ferramenta para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar a `audit-sum` ferramenta para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

Informações relacionadas

[Utilize a ferramenta de auditoria-explicação](#)

[Use a ferramenta `audit-sum`](#)

Utilize a ferramenta de auditoria-explicação

Você pode usar a `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria em um formato fácil de ler.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-explain` ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.



A `audit-explain` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-explain` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-explain` ferramenta. Essas quatro mensagens de auditoria do SPUT foram geradas quando o locatário S3 com ID de conta 92484777680322627870 usou S3 SOLICITAÇÕES PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

A `audit-explain` ferramenta pode processar logs de auditoria simples ou compactados. Por exemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

A `audit-explain` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Finalmente, a `audit-explain` ferramenta pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando partes que você deseja olhar e executar `audit-explain` nas partes, em vez de todo o arquivo.



A `audit-explain` ferramenta não aceita arquivos compactados como entrada pipeada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:

```
zcat audit.log.gz | audit-explain
```

Utilize a `help` (`-h`) opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Faça login no nó de administração principal:
 - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

```
$ audit-explain /var/local/audit/export/audit.log
```

A `audit-explain` ferramenta imprime interpretações humanamente legíveis de todas as mensagens no arquivo ou arquivos especificados.



Para reduzir o comprimento das linhas e facilitar a legibilidade, os carimbos de data/hora não são apresentados por predefinição. Se você quiser ver os carimbos de data/hora, use a opção carimbo de data/hora (`-t`).

Informações relacionadas

[SPUT: S3 PUT](#)

Use a ferramenta `audit-sum`

Você pode usar a `audit-sum` ferramenta para contar as mensagens de auditoria de

gravação, leitura, cabeçalho e exclusão e ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

Sobre esta tarefa

A `audit-sum` ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.



A `audit-sum` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-sum` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
message group          count      min(sec)      max(sec)
average(sec)
=====
=====
=====
=====
IDEL                   274
SDEL                   213371      0.004         20.934
0.352
SGET                   201906      0.010         1740.290
1.132
SHEA                   22716       0.005         2.349
0.272
SPUT                   1771398     0.011         1770.563
0.487
```

A `audit-sum` ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria S3, Swift e ILM em um log de auditoria:

Código	Descrição	Consulte
ARCT	Recuperação de arquivamento do Cloud-Tier	ARCT: Recuperação de arquivos do Cloud-Tier
ASCT	Archive Store Cloud-Tier	ASCT: Archive Store Cloud-Tier
IDEL	ILM iniciado Excluir: Registra quando ILM inicia o processo de exclusão de um objeto.	IDEL: ILM iniciou Excluir

Código	Descrição	Consulte
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket.	SDEL: S3 DELETE
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	SGET: S3 GET
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	SHEA: S3 CABEÇA
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	SPUT: S3 PUT
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	WDEL: Swift DELETE
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	WGET: Rápido
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	WHEA: CABEÇA rápida
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	WPUT: Swift PUT

A `audit-sum` ferramenta pode processar logs de auditoria simples ou compactados. Por exemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

A `audit-sum` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Finalmente, a `audit-sum` ferramenta também pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Esta ferramenta não aceita arquivos compactados como entrada pipeada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Você pode usar as opções de linha de comando para resumir as operações em intervalos separadamente das operações em objetos ou agrupar resumos de mensagens por nome de intervalo, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo de operação mínimo, máximo e médio, mas você pode usar a `size (-s)` opção para olhar o tamanho do objeto.

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Faça login no nó de administração principal:
 - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
 - a. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

```
$ audit-sum /var/local/audit/export/audit.log
```

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as

operações de protocolo demoraram.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

Neste exemplo, as operações de SGET (S3 GET) são as mais lentas em média em 1,13 segundos, mas as operações de SGET e SPUT (S3 PUT) mostram tempos piores longos de cerca de 1.770 segundos.

- b. Para mostrar as operações de recuperação 10 mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicionar a opção de saída longa (-l) para incluir caminhos de objeto:
grep SGET audit.log | audit-sum -l

Os resultados incluem o tipo (objeto ou bucket) e o caminho, que permite que você grep o log de auditoria para outras mensagens relacionadas a esses objetos específicos.


```

Total:          201906 operations
Slowest:       1740.290 sec
Average:       1.132 sec
Fastest:       0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====      =====      =====      =====      =====
      1740289662    10.96.101.125      object    5663711385
backup/r9010aQ8JB-1566861764-4519.iso
      1624414429    10.96.101.125      object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793    10.96.101.125      object    5183661466
backup/r9010aQ8JB-1566861764-4518.iso
      70839         10.96.101.125      object     28338
bucket3/dat.1566861764-6619
      68487         10.96.101.125      object     27890
bucket3/dat.1566861764-6615
      67798         10.96.101.125      object     27671
bucket5/dat.1566861764-6617
      67027         10.96.101.125      object     27230
bucket5/dat.1566861764-4517
      60922         10.96.101.125      object     26118
bucket3/dat.1566861764-4520
      35588         10.96.101.125      object     11311
bucket3/dat.1566861764-6616
      23897         10.96.101.125      object     10692
bucket3/dat.1566861764-4516

```

+ A partir deste exemplo de saída, você pode ver que os três pedidos mais lentos de S3 GET foram para objetos de tamanho de cerca de 5 GB, que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos do pior caso.

3. Se você quiser determinar em que tamanhos de objetos estão sendo ingeridos e recuperados da grade, use a opção tamanho (-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior do que o número de mensagens SGET, indicando que a maioria dos objetos nunca são recuperados.

4. Se você quiser determinar se as recuperações foram lentas ontem:

- a. Emita o comando no log de auditoria apropriado e use a opção Group-by-time (-gt), seguida pelo período de tempo (por exemplo, 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Esses resultados mostram que S3 RECEBEM tráfego aumentado entre 06:00 e 07:00. Os tempos máximos e médios são consideravelmente mais elevados nestes tempos também, e eles não aumentaram gradualmente à medida que a contagem aumentou. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

- b. Para determinar que objetos de tamanho estavam sendo recuperados a cada hora ontem, adicione a opção tamanho (-s) ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no seu máximo.

- c. Para ver mais detalhes, use a `audit-explain` ferramenta para revisar todas as operações SGET durante essa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando `grep` for esperada para ser muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) de cada vez.

- 5. Se você quiser determinar se as operações do SPUT em buckets são mais lentas do que as operações do SPUT para objetos:
 - a. Comece usando a `-go` opção, que agrupa as mensagens para operações de objeto e bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.bucket	1	0.125	0.125
0.125			
SPUT.object	12	0.025	1.019
0.236			

Os resultados mostram que as operações do SPUT para buckets têm características de desempenho diferentes das operações do SPUT para objetos.

- b. Para determinar quais buckets têm as operações de SPUT mais lentas, use a `-gb` opção, que agrupa as mensagens por bucket:

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	0.046	1770.563
1.571			
SPUT.cho-versioning	54277	0.047	1736.633
1.415			
SPUT.cho-west-region	80615	0.040	55.557
1.329			
SPUT.ldt002	1564563	0.011	51.569
0.361			

- c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use as `-gb` opções e `-s`:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group	count	min (B)	max (B)
average (B)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	2.097	5000.000
21.672			
SPUT.cho-versioning	54277	2.097	5000.000
21.120			
SPUT.cho-west-region	80615	2.097	800.000
14.433			
SPUT.ltd002	1564563	0.000	999.972
0.352			

Informações relacionadas

[Utilize a ferramenta de auditoria-explicação](#)

Formato da mensagem de auditoria

As mensagens de auditoria trocadas no sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou a atividade que está sendo relatada.

Se as informações resumidas fornecidas pelas `audit-explain` ferramentas e `audit-sum` forem insuficientes, consulte esta secção para compreender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Cada mensagem de auditoria contém uma cadeia de elementos de atributo. Toda a cadeia de caracteres está entre colchetes ([]), e cada elemento de atributo na cadeia de caracteres tem as seguintes características:

- Entre os suportes []
- Introduzido pela cadeia de caracteres `AUDT`, que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de alimentação de linha `\n`

Cada elemento inclui um código de atributo, um tipo de dados e um valor que são relatados neste formato:

```
[ATTR (type) :value] [ATTR (type) :value] ...  
[ATTR (type) :value] \n
```

O número de elementos de atributo na mensagem depende do tipo de evento da mensagem. Os elementos de atributo não são listados em nenhuma ordem específica.

A lista a seguir descreve os elementos do atributo:

- `ATTR` é um código de quatro caracteres para o atributo que está sendo relatado. Existem alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos para eventos.
- `type` É um identificador de quatro caracteres do tipo de dados de programação do valor, como `UI64`, `FC32` e assim por diante. O tipo está entre parênteses ().
- `value` é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores seguem sempre dois pontos (:). Os valores do tipo de dados `CSTR` são cercados por aspas "" duplas .

Informações relacionadas

[Utilize a ferramenta de auditoria-explicação](#)

[Use a ferramenta audit-sum](#)

[Auditar mensagens](#)

[Elementos comuns em mensagens de auditoria](#)

[Tipos de dados](#)

[Exemplos de mensagens de auditoria](#)

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo não assinado (32 bits); ele pode armazenar os números de 0 a 4.294.967.295.
UI64	Número inteiro duplo longo não assinado (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro caracteres; um valor inteiro não assinado de 32 bits representado como quatro caracteres ASCII, como "ABCD".
IPAD	Usado para endereços IP.

Tipo	Descrição
CSTR	<p>Um array de comprimento variável de caracteres UTF-8. Os caracteres podem ser escapados com as seguintes convenções:</p> <ul style="list-style-type: none"> • Barra invertida é. • O retorno do carro é r. • Aspas duplas. • A alimentação de linha (nova linha) é n. • Os caracteres podem ser substituídos por seus equivalentes hexadecimais (no formato HH, onde HH é o valor hexadecimal que representa o caractere).

Dados específicos do evento

Cada mensagem de auditoria no log de auditoria Registra dados específicos para um evento do sistema.

Após o conteúdo de abertura [AUDT: que identifica a própria mensagem, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrito pela mensagem de auditoria. Esses atributos são destacados no exemplo a seguir:

```
2018 11454 S3AI SGKH4 60025621595611246499 UI64-12 10.224.0 60025621595611246499
E6DYZKLUMRSKJA S3BK-05T08:24 100 S3AK 60025621595611246499 S3KY
[AUDT:*[RSLT(FC32):SUCS]* *[TIME STR(UI64):45,921845 E4DA UI64 30720 UI32 10 UI64
1543998285921845 FC32 UI32 12281045 FC32 S3RQ UI64 15552417629170647261
```

O **ATYP** elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o código de mensagem SHEA ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

Informações relacionadas

[Elementos comuns em mensagens de auditoria](#)

[Auditar mensagens](#)

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
NO MEIO	FC32	ID do módulo: Um identificador de quatro caracteres do ID do módulo que gerou a mensagem. Isso indica o segmento de código no qual a mensagem de auditoria foi gerada.

Código	Tipo	Descrição
ANID	UI32	ID do nó: O ID do nó da grade atribuído ao serviço que gerou a mensagem. Cada serviço recebe um identificador exclusivo no momento em que o sistema StorageGRID é configurado e instalado. Este ID não pode ser alterado.
ASES	UI64	Identificador de sessão de auditoria: Em versões anteriores, este elemento indicou o momento em que o sistema de auditoria foi inicializado após o início do serviço. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Nota: este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: Em versões anteriores, esse contador foi incrementado para cada mensagem de auditoria gerada no nó de grade (ANID) e redefinido para zero na reinicialização do serviço. Nota: este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: Um identificador que é compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.
ATIM	UI64	Timestamp: A hora em que o evento foi gerado, que acionou a mensagem de auditoria, medida em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora para data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o carimbo de data/hora registado. O tempo legível por humanos que aparece no início da mensagem de auditoria no <code>audit.log</code> arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> , onde o <code>T</code> é um caractere de cadeia de caracteres literal indicando o início do segmento de tempo da data. <code>UUUUUU</code> são microssegundos.
ATYP	FC32	Tipo de evento: Um identificador de quatro caracteres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: Os atributos que estão incluídos.
AVER	UI32	Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade retroativa no serviço AMS para processar mensagens de versões mais antigas de serviços.
RSLT	FC32	Resultado: O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente.

Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está uma mensagem de auditoria de exemplo, como ela pode aparecer no `audit.log` arquivo:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK (CSTR) : "s3small11" ] [S3K
Y (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0
] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP (FC32) :SPUT
] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :1579224144
102530435]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo gravado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é gravado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK (CSTR) : "s3small11" ] [S3K
Y (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0
] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP \ (FC32) : SPU
T] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :1579224
144102530435]]
```

O valor do atributo ATYP é SPUT. O SPUT representa uma transação S3 PUT, que Registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o intervalo ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f" ] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2" ] [S3BK \ (CSTR) : "s3small11" ] [S3
KY (CSTR) : "hello1" ] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :
0] [AVER (UI32) :10] [ATIM (UI64) :1405631878959669] [ATYP (FC32) :SPU
T] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :157922414
4102530435]]
```

Para descobrir quando o evento PUT ocorreu, observe o carimbo de data/hora Universal coordenada (UTC) no início da mensagem de auditoria. Este valor é uma versão legível por humanos do atributo ATIM da própria mensagem de auditoria:

2014-07-17T21:17:58.959669

```
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2"] [S3BK (CSTR) : "s3small11"] [S3KY (CSTR) : "hello1"] [CBID (UI64) :0x50C4F7AC2BC8EDF7] [CSIZ (UI64) :0] [AVER (UI32) :10] [ATIM\ (UI64\ ) :1405631878959669] [ATYP (FC32) :SPUT] [ANID (UI32) :12872812] [AMID (FC32) :S3RQ] [ATID (UI64) :1579224144102530435]]
```

ATIM Registra o tempo, em microssegundos, desde o início da época UNIX. No exemplo, o valor 1405631878959669 é traduzido para Quinta-feira, 17-Jul-2014 21:17:59 UTC.

Informações relacionadas

[SPUT: S3 PUT](#)

[Elementos comuns em mensagens de auditoria](#)

Auditar mensagens e o ciclo de vida do objeto

As mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API (S3 ou Swift).

As mensagens de auditoria são vinculadas por meio de identificadores específicos a cada protocolo.

Protocolo	Código
Ligar S3 operações	S3BK (balde S3) e/ou S3KY (chave S3)
Ligando as operações Swift	WCON (Swift Container) e/ou WOBJ (Swift Object)
Vinculação de operações internas	CBID (Identificador Interno do Objeto)

Calendário das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós de grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar da mostrada nos exemplos nesta seção.

Configuração da política de gerenciamento do ciclo de vida das informações

Com a política ILM padrão (cópia de linha de base 2), os dados do objeto são copiados uma vez para um total de duas cópias. Se a política ILM exigir mais de duas cópias, haverá um conjunto adicional de mensagens CBRE, CBSE e SCMT para cada cópia extra. Para obter mais informações sobre políticas de ILM, consulte informações sobre como gerenciar objetos com gerenciamento do ciclo de vida das informações.

Nós de arquivamento

A série de mensagens de auditoria geradas quando um nó de arquivo envia dados de objeto para um sistema de armazenamento de arquivo externo é semelhante à dos nós de armazenamento, exceto que não há mensagem SCMT (Store Object Commit), e as mensagens ATCE (Archive Object Store Begin) e ASCE (Archive Object Store End) são geradas para cada cópia arquivada de dados de objeto.

A série de mensagens de auditoria geradas quando um nó de arquivo recupera dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que as mensagens ARCB (recuperação de objetos de arquivamento iniciada) e ARCE (fim de recuperação de objetos de arquivamento) são geradas para cada cópia recuperada de dados de objetos.

A série de mensagens de auditoria geradas quando um nó de arquivo exclui dados de objetos de um sistema de armazenamento de arquivos externo é semelhante à dos nós de armazenamento, exceto que não há nenhuma mensagem SREM (Object Store Remove) e há uma mensagem AREM (Archive Object Remove) para cada solicitação de exclusão.

Informações relacionadas

[Gerenciar objetos com ILM](#)

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API (S3 ou Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de ingestão são incluídas.

S3 ingira mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SPUT	S3 COLOQUE a transação	Uma transação de ingestão de S3 PUT foi concluída com sucesso.	CBID, S3BK, S3KY	SPUT: S3 PUT
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	ORLM: Regras Objeto cumpridas

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Traçado	Consulte
WPUT	Transação de COLOCAÇÃO rápida	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBID, WCON, WOBJ	WPUT: Swift PUT

Código	Nome	Descrição	Traçado	Consulte
ORLM	Regras Objeto cumpridas	A política ILM foi satisfeita para este objeto.	CBID	ORLM: Regras Objeto cumpridas

Exemplo: Ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente S3 ingere um objeto em um nó de armazenamento (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM de estoque, faça 2 cópias.



Nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de ingestão S3 (SPUT) estão listados.

Este exemplo assume que um bucket do S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um intervalo específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]
```

ORLM: Regras Objeto cumpridas

A mensagem ORLM indica que a política ILM foi satisfeita para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume das localizações do objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Para objetos codificados por apagamento, o campo LOCS inclui o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contentor e objeto do Swift, dependendo de qual API foi usada.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Eliminar transações

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de exclusão são incluídas.

S3 exclua mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
SDEL	S3 Eliminar	Solicitação feita para excluir o objeto de um intervalo.	CBID, S3KY	SDEL: S3 DELETE

Swift delete mensagens de auditoria

Código	Nome	Descrição	Traçado	Consulte
WDEL	Eliminação rápida	Solicitação feita para excluir o objeto de um recipiente ou do recipiente.	CBID, WOBJ	WDEL: Swift DELETE

Exemplo: Exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.



Nem todas as mensagens de auditoria geradas durante uma transação de exclusão são listadas no exemplo abaixo. Apenas os relacionados com a transação de exclusão S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objeto começa quando o cliente envia uma solicitação DE EXCLUSÃO de objeto para um serviço LDR. A mensagem contém o intervalo do qual excluir o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\CSTR\):"example"\\[S3KY\CSTR\):"testobject-0-
7"\][CBID(UI64):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP(FC32):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]
```

Recuperar transações objeto

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API (S3 e Swift).

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação são listadas nas tabelas a seguir. Apenas as mensagens necessárias para rastrear a transação de recuperação são incluídas.

S3 mensagens de auditoria de recuperação

Código	Nome	Descrição	Traçado	Consulte
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBID, S3BK, S3KY	SGET: S3 GET

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Traçado	Consulte
WGET	Swift GET	Solicitação feita para recuperar um objeto de um contentor.	CBID, WCON, WOBJ	WGET: Rápido

Exemplo: Recuperação de objeto S3D.

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Apenas os relacionados à transação de recuperação S3 (SGET) estão listados.

SGET: S3 GET

A recuperação de objetos começa quando o cliente envia uma SOLICITAÇÃO GET Object a um serviço LDR. A mensagem contém o intervalo do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificar o objeto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-a"][S3AK(CSTR):"SGKht7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]\[S3BK\CSTR\):"bucket-anonymous"\]\[S3KY\CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\) :SGET\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política de bucket permitir, um cliente pode recuperar objetos anonimamente ou recuperar objetos de um bucket que é de propriedade de uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta de locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma SOLICITAÇÃO GET Object para um objeto armazenado em um bucket que ele não possui. Os valores para SBAI e SBAC registram o ID e o nome da conta do locatário do proprietário do bucket, que difere do ID da conta do locatário e do nome do cliente registrado em S3AI e SACC.


```
2017-09-20T22:53:15.876415
```

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI\n(CSTR):"17915054115450519830"\]\[SACC(CSTR):"s3-account-b"\]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="\]\[SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"\]\[SBAI\n(CSTR):"43979298178977966408"\]\[SBAC(CSTR):"s3-account-a"\]\[S3BK(CSTR):"bucket-anonymous"\]\[S3KY(CSTR):"Hello.txt"\]\[CBID(UI64):0x83D70C6F1F662B02]\[CSIZ(UI64):12]\[AVER(UI32):10]\[ATIM(UI64):1505947995876415]\[ATYP(FC32):SGET]\[ANID(UI32):12272050]\[AMID(FC32):S3RQ]\[ATID(UI64):6888780247515624902]]
```

Exemplo: S3 Seleção em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, as mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação são listadas no exemplo abaixo. Somente aqueles relacionados à transação S3 Select (SelectObjectContent) são listados.

Cada consulta resulta em duas mensagens de auditoria: Uma que executa a autorização da solicitação Select S3 (o campo S3SR está definido como "select") e uma operação GET padrão subsequente que recupera os dados do armazenamento durante o processamento.

```
2021-11-08T15:35:30.750038
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAIP(IPAD):"192.168.7.44"]\[S3AI(CSTR):"63147909414576125820"\]\[SACC(CSTR):"Tenant1636027116"\]\[S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"\]\[SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"\]\[SBAI(CSTR):"63147909414576125820"\]\[SBAC(CSTR):"Tenant1636027116"\]\[S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"\]\[S3KY(CSTR):"SUB-EST2020_ALL.csv"\]\[CBID(UI64):0x0496F0408A721171]\[UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"\]\[CSIZ(UI64):0]\[S3SR(CSTR):"select"\]\[AVER(UI32):10]\[ATIM(UI64):1636385730750038]\[ATYP(FC32):SPOS]\[ANID(UI32):12601166]\[AMID(FC32):S3RQ]\[ATID(UI64):1363009709396895985]]
```

2021-11-08T15:35:32.604886

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\": \"unix:\"}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant1636027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identity:63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CSTR):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"] [S3KY(CSTR):"SUB-EST2020_ALL.csv"] [CBID(UI64):0x0496F0408A721171] [UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"] [CSIZ(UI64):10185581] [MTME(UI64):1636380348695262] [AVER(UI32):10] [ATIM(UI64):1636385732604886] [ATYP(FC32):SGET] [ANID(UI32):12733063] [AMID(FC32):S3RQ] [ATID(UI64):16562288121152341130]]
```

Mensagens de atualização de metadados

As mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados do S3

Código	Nome	Descrição	Traçado	Consulte
SUPD	S3 metadados atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBID, S3KY, HTRH	SUPD: S3 metadados atualizados

Exemplo: Atualização de metadados S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: Atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados (`x-amz-meta-*`) para o objeto S3 (S3KY). Neste exemplo, cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO > Monitoramento > Auditoria e servidor syslog**).

```

2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrDplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]

```

Informações relacionadas

[Configurar mensagens de auditoria e destinos de log](#)

Auditar mensagens

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema são listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiramente em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas alfabeticamente por seus códigos de quatro caracteres. Esta lista alfabética permite-lhe encontrar informações sobre mensagens específicas.

Os códigos de quatro caracteres utilizados ao longo deste capítulo são os valores ATYP encontrados nas mensagens de auditoria, conforme mostrado na seguinte mensagem de exemplo:

```

2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]

```

Para obter informações sobre como definir níveis de mensagens de auditoria, alterar destinos de log e usar

um servidor syslog externo para suas informações de auditoria, consulte [Configurar mensagens de auditoria e destinos de log](#)

Auditar categorias de mensagens

Você deve estar familiarizado com as várias categorias nas quais as mensagens de auditoria são agrupadas. Esses grupos são organizados com base na classe de atividade que a mensagem representa.

Mensagens de auditoria do sistema

Você deve estar familiarizado com as mensagens de auditoria pertencentes à categoria de auditoria do sistema. Esses são eventos relacionados ao próprio sistema de auditoria, estados de nó de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço, para que você possa lidar com possíveis problemas.

Código	Título e descrição da mensagem	Consulte
ECMC	Fragmento de dados codificado de apagamento ausente: Indica que um fragmento de dados codificado de apagamento ausente foi detetado.	ECMC: Fragmento de dados codificados de apagamento em falta
ECOC	Fragmento de dados codificado de apagamento corrompido: Indica que um fragmento de dados codificado de apagamento corrompido foi detetado.	ECOC: Fragmento de dados codificado de apagamento corrompido
ETAF	Falha na autenticação de segurança: Uma tentativa de conexão usando TLS (Transport Layer Security) falhou.	ETAF: Falha na autenticação de segurança
GNRG	Registro GNDS: Um serviço atualizado ou registrado informações sobre si mesmo no sistema StorageGRID.	GNRG: Registro GNDS
GNUR	GNDS Unregistration: Um serviço não se registrou a partir do sistema StorageGRID.	GNUR: GNDS Unregistration
GTED	Tarefa de grelha terminada: O serviço CMN terminou de processar a tarefa de grelha.	GTED: Tarefa de grelha terminada

Código	Título e descrição da mensagem	Consulte
GTST	Tarefa de grade iniciada: O serviço CMN começou a processar a tarefa de grade.	GTST: Tarefa de grade iniciada
GTSU	Tarefa de grelha enviada: Uma tarefa de grelha foi enviada para o serviço CMN.	GTSU: Tarefa de grelha enviada
IDEL	Exclusão iniciada ILM: Esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	IDEL: ILM iniciou Excluir
LKCU	Limpeza Objeto sobrescrita. Esta mensagem de auditoria é gerada quando um objeto substituído é removido automaticamente para liberar espaço de armazenamento.	LKCU: Limpeza de objetos sobrescritos
LLST	Localização perdida: Esta mensagem de auditoria é gerada quando um local é perdido.	LLST: Localização perdida
OLST	Objeto perdido: Um objeto solicitado não pode ser localizado dentro do sistema StorageGRID.	OLST: O sistema detetou Objeto perdido
ORLM	Regras do objeto atendidas: Os dados do objeto são armazenados conforme especificado pelas regras do ILM.	ORLM: Regras Objeto cumpridas
ADICIONAR	Desativação da auditoria de segurança: O registo de mensagens de auditoria foi desativado.	ADICIONAR: Desativação da auditoria de segurança
SADE	Ativação da auditoria de segurança: O registo de mensagens de auditoria foi restaurado.	SADE: Ativação da auditoria de segurança
SVRF	Falha na verificação do armazenamento de objetos: Um bloco de conteúdo falhou verificações.	SVRF: Falha na verificação do armazenamento de objetos

Código	Título e descrição da mensagem	Consulte
SVRU	Verificação desconhecido: Dados de objeto inesperados detetados no armazenamento de objetos.	SVRU: Verificação do armazenamento de objetos desconhecido
SYSD	Paragem nó: Foi solicitado um encerramento.	SYSD: Parada do nó
SIST	Parada do nó: Um serviço iniciou uma parada graciosa.	SIST: Paragem do nó
SYSU	Início do nó: Um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	SYSU: Início do nó
VLST	Volume perdido iniciado pelo usuário: O <code>/proc/CMSI/Volume_Lost</code> comando foi executado.	VLST: Volume iniciado pelo usuário perdido

Informações relacionadas

[LKCU: Limpeza de objetos sobrescritos](#)

Mensagens de auditoria de armazenamento de objetos

Você deve estar familiarizado com as mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos. Estes são eventos relacionados ao armazenamento e gerenciamento de objetos no sistema StorageGRID. Isso inclui armazenamento de objetos e recuperações, transferências de nó de grade para nó de grade e verificações.

Código	Descrição	Consulte
APCT	Limpeza de arquivamento da camada da nuvem: Os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	APCT: Purga de arquivamento do nível de nuvem
ARCB	Início da recuperação de objetos de arquivamento: O serviço ARC inicia a recuperação de dados de objetos do sistema de armazenamento de arquivos externo.	ARCB: Início da recuperação de objetos de arquivamento

Código	Descrição	Consulte
ARCE	Fim de recuperação de objetos de arquivamento: Os dados de objetos foram recuperados de um sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de recuperação.	ARCE: Fim de recuperação de objetos de arquivamento
ARCT	Recuperação de arquivos do Cloud-Tier: Os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	ARCT: Recuperação de arquivos do Cloud-Tier
ACEM	Remoção de objeto de arquivamento: Um bloco de conteúdo foi excluído com sucesso ou sem sucesso do sistema de armazenamento de arquivos externo.	AFEM: Remoção de objetos de Arquivo
ASCE	Fim do armazenamento de objetos de arquivamento: Um bloco de conteúdo foi gravado no sistema de armazenamento de arquivos externo e o serviço ARC relata o status da operação de gravação.	ASCE: Fim do armazenamento de objetos de Arquivo
ASCT	Camada de nuvem: Os dados de objetos são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.	ASCT: Archive Store Cloud-Tier
ATCE	Início do armazenamento de objetos de arquivamento: A gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.	ATCE: Início do armazenamento de objetos de arquivo
AVCC	Archive Validate Cloud-Tier Configuration: As configurações de conta e bucket fornecidas foram validadas com êxito ou sem sucesso.	AVCC: Arquivamento Validar Configuração de nível de nuvem

Código	Descrição	Consulte
CBSE	Fim de envio de objeto: A entidade de origem concluiu uma operação de transferência de dados de nó de grade para nó de grade.	CBSE: Fim de envio de objeto
CBRE	Fim de recebimento de objeto: A entidade de destino concluiu uma operação de transferência de dados de nó de grade para nó de grade.	CBRE: Fim de recebimento do objeto
SCMT	Object Store commit: Um bloco de conteúdo foi completamente armazenado e verificado, e agora pode ser solicitado.	SCMT: Confirmação de armazenamento de objetos
SREM	Remoção do armazenamento de objetos: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	SREM: Armazenamento de objetos Remover

O cliente lê mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. Nota: se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	SGET: S3 GET
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	SHEA: S3 CABEÇA

Código	Descrição	Usado por	Consulte
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	Cliente Swift	WGET: Rápido
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	Cliente Swift	WHEA: CABEÇA rápida

O cliente escreve mensagens de auditoria

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 ou Swift faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Consulte
OVWR	Object Overwrite: Registra uma transação para sobrescrever um objeto com outro objeto.	S3 clientes Clientes Swift	OVWR: Substituição de objetos
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket. Nota: se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	SDEL: S3 DELETE
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	SPOS: S3 POST

Código	Descrição	Usado por	Consulte
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket. Nota: se a transação operar em um subrecurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	SPUT: S3 PUT
SUPD	S3 metadados atualizados: Registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	SUPD: S3 metadados atualizados
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	Cliente Swift	WDEL: Swift DELETE
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	Cliente Swift	WPUT: Swift PUT

Mensagem de auditoria de gerenciamento

A categoria Gerenciamento Registra as solicitações do usuário para a API de gerenciamento.

Código	Título e descrição da mensagem	Consulte
MGAU	Mensagem de auditoria da API de gerenciamento: Um log de solicitações de usuário.	MGAU: Mensagem de auditoria de gestão

Referência da mensagem de auditoria

APCT: Purga de arquivamento do nível de nuvem

Essa mensagem é gerada quando os dados de objetos arquivados são excluídos de um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi excluído.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. Sempre retorna 0.
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem do qual o objeto foi excluído.

ARCB: Início da recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma solicitação é feita para recuperar dados de objetos arquivados e o processo de recuperação é iniciado. Os pedidos de recuperação são processados imediatamente, mas podem ser reordenados para melhorar a eficiência da recuperação de meios lineares, como fita.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.
RSLT	Resultado	Indica o resultado do início do processo de recuperação do arquivo. O valor atualmente definido é:SUCS: A solicitação de conteúdo foi recebida e enfileirada para recuperação.

Esta mensagem de auditoria marca a hora de uma recuperação de arquivo. Ele permite que você combine a mensagem com uma mensagem final ARCE correspondente para determinar a duração da recuperação do arquivo e se a operação foi bem-sucedida.

ARCE: Fim de recuperação de objetos de arquivamento

Esta mensagem é gerada quando uma tentativa do nó de arquivo para recuperar dados de objetos de um sistema de armazenamento de arquivos externo é concluída. Se for bem-sucedida, a mensagem indica que os dados do objeto solicitado foram completamente lidos a partir do local do arquivo e foram verificados com sucesso. Depois que os dados do objeto forem recuperados e verificados, eles serão entregues ao serviço solicitante.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de armazenamento de arquivos externo.
VLID	Identificador de volume	O identificador do volume no qual os dados foram arquivados. se não for encontrada uma localização de arquivo para o conteúdo, é devolvida uma ID de volume de 0.
RSLT	Resultado de recuperação	O estado de conclusão do processo de recuperação do arquivo: <ul style="list-style-type: none"> • SUCS: Bem-sucedido • VRFL: Falhou (falha na verificação de objetos) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • CANC: Falha (operação de recuperação cancelada) • GERR: Falhou (erro geral)

A correspondência desta mensagem com a mensagem ARCB correspondente pode indicar o tempo necessário para executar a recuperação do arquivo. Esta mensagem indica se a recuperação foi bem-sucedida e, em caso de falha, a causa da falha na recuperação do bloco de conteúdo.

ARCT: Recuperação de arquivos do Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são recuperados de um sistema de armazenamento de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes. O valor só é preciso para recuperações bem-sucedidas.

Código	Campo	Descrição
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador único (UUID) do sistema de armazenamento de arquivos externo.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

AFEM: Remoção de objetos de Arquivo

A mensagem de auditoria Remove Objeto de Arquivo indica que um bloco de conteúdo foi excluído com sucesso ou sem sucesso de um nó de Arquivo. Se o resultado for bem-sucedido, o nó de arquivo informou com sucesso o sistema de armazenamento de arquivamento externo de que o StorageGRID liberou um local de objeto. Se o objeto é removido do sistema de armazenamento de arquivos externo depende do tipo de sistema e sua configuração.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser recuperado do sistema de Mídia de arquivamento externo.
VLID	Identificador de volume	O identificador do volume no qual os dados do objeto foram arquivados.
RSLT	Resultado	O estado de conclusão do processo de remoção do arquivo: <ul style="list-style-type: none"> • SUCS: Bem-sucedido • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

ASCE: Fim do armazenamento de objetos de Arquivo

Esta mensagem indica que a gravação de um bloco de conteúdo em um sistema de armazenamento de arquivos externo terminou.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador do bloco de conteúdo armazenado no sistema de armazenamento de arquivos externo.
VLID	Identificador de volume	O identificador exclusivo do volume de arquivo no qual os dados do objeto são gravados.
VREN	Verificação ativada	Indica se a verificação é realizada para blocos de conteúdo. Os valores atualmente definidos são: <ul style="list-style-type: none"> • VENA: A verificação está ativada • VDSA: A verificação está desativada
MCLS	Classe de Gestão	Uma cadeia de caracteres que identifica a classe de gerenciamento TSM à qual o bloco de conteúdo é atribuído, se aplicável.
RSLT	Resultado	Indica o resultado do processo de arquivo. Os valores atualmente definidos são: <ul style="list-style-type: none"> • SUCS: Bem-sucedido (processo de arquivamento bem-sucedido) • OFFL: Falhou (o arquivamento está offline) • VRFL: Falhou (verificação de objeto falhou) • ARUN: Falhou (sistema de armazenamento de arquivamento externo indisponível) • GERR: Falhou (erro geral)

Esta mensagem de auditoria significa que o bloco de conteúdo especificado foi gravado no sistema de armazenamento de arquivos externo. Se a gravação falhar, o resultado fornece informações básicas de solução de problemas sobre onde a falha ocorreu. Informações mais detalhadas sobre falhas de arquivo podem ser encontradas examinando os atributos do nó de arquivo no sistema StorageGRID.

ASCT: Archive Store Cloud-Tier

Essa mensagem é gerada quando os dados de objetos arquivados são armazenados em um sistema de storage de arquivamento externo, que se conecta ao StorageGRID por meio da API S3.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo para o bloco de conteúdo que foi recuperado.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
RSLT	Código do resultado	Retorna bem-sucedido (SUCC) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	Identificador exclusivo (UUID) do nível de nuvem para o qual o conteúdo foi armazenado.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

ATCE: Início do armazenamento de objetos de arquivo

Essa mensagem indica que a gravação de um bloco de conteúdo em um armazenamento de arquivamento externo foi iniciada.

Código	Campo	Descrição
CBID	ID do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo a ser arquivado.
VLID	Identificador de volume	O identificador exclusivo do volume para o qual o bloco de conteúdo é escrito. Se a operação falhar, um ID de volume de 0 é retornado.

Código	Campo	Descrição
RSLT	Resultado	Indica o resultado da transferência do bloco de conteúdo. Os valores atualmente definidos são: <ul style="list-style-type: none"> • SUCS: Sucesso (bloco de conteúdo armazenado com sucesso) • EXIS: Ignorado (bloco de conteúdo já estava armazenado) • ISFD: Falha (espaço em disco insuficiente) • STER: Falhou (erro ao armazenar o CBID) • OFFL: Falhou (o arquivamento está offline) • GERR: Falhou (erro geral)

AVCC: Arquivamento Validar Configuração de nível de nuvem

Essa mensagem é gerada quando as configurações são validadas para um tipo de destino Cloud Tiering - Simple Storage Service (S3).

Código	Campo	Descrição
RSLT	Código do resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.
SUID	Identificador exclusivo de armazenamento	UUID associado ao sistema de armazenamento de arquivamento externo sendo validado.

CBRB: Início de recebimento de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBRE: Fim de recebimento do objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.

Código	Campo	Descrição
RSLT	Resultado da transferência	<p>O resultado da operação de transferência (do ponto de vista da entidade de envio):</p> <p>SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas.</p> <p>CONL: Conexão perdida durante a transferência</p> <p>CTMO: Tempo limite de conexão durante o estabelecimento ou transferência</p> <p>UNRE: ID do nó de destino inalcançável</p> <p>CRPT: Transferência terminada devido à recepção de dados corrompidos ou inválidos (pode indicar adulteração)</p>

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objetos

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre nós diferentes à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se for bem-sucedida, a transferência começa a partir desta contagem de sequência.
CTES	Contagem sequência fim esperado	Indica a última contagem de sequência solicitada. Se for bem-sucedida, a transferência é considerada concluída quando esta contagem de sequência tiver sido recebida.
RSLT	Estado Início transferência	Estado no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Essa mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único conteúdo, conforme identificado por seu Identificador de bloco de conteúdo. A operação solicita dados de "Start Sequence Count" (contagem de sequência de início) para "expected End Sequence Count" (contagem de sequência de fim esperado) Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBSE: Fim de envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro for concluída, essa mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador exclusivo da sessão/conexão nó a nó.
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou iniciada por pull: PUSH: A operação de transferência foi solicitada pela entidade emissora. PULL: A operação de transferência foi solicitada pela entidade recetora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de destino	O ID do nó do destino (recetor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência com a qual a transferência foi iniciada.
CTAS	Contagem sequência fim Real	Indica a última contagem de sequência transferida com êxito. Se a contagem de sequência final real for a mesma que a contagem de sequência inicial e o resultado da transferência não tiver sido bem-sucedido, não foram trocados dados.

Código	Campo	Descrição
RSLT	Resultado da transferência	<p>O resultado da operação de transferência (do ponto de vista da entidade de envio):</p> <p>SUCS: Transferência concluída com êxito; todas as contagens de sequência solicitadas foram enviadas.</p> <p>CONL: Conexão perdida durante a transferência</p> <p>CTMO: Tempo limite de conexão durante o estabelecimento ou transferência</p> <p>UNRE: ID do nó de destino inalcançável</p> <p>CRPT: Transferência terminada devido à recepção de dados corrompidos ou inválidos (pode indicar adulteração)</p>

Essa mensagem de auditoria significa que uma operação de transferência de dados nó a nó foi concluída. Se o resultado da transferência tiver sido bem-sucedido, a operação transferiu dados de "Start Sequence Count" (contagem de sequência de início) para "Real End Sequence Count" (contagem de sequência final real). Os nós de envio e recebimento são identificados por suas IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, ele também pode ser usado para verificar contagens de réplicas.

ECMC: Fragmento de dados codificados de apagamento em falta

Esta mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento em falta.

Código	Campo	Descrição
VCMC	ID VCS	O nome do VCS que contém o pedaço em falta.
MCID	Código bloco	O identificador do fragmento codificado de apagamento em falta.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificado de apagamento corrompido

Essa mensagem de auditoria indica que o sistema detetou um fragmento de dados codificado de apagamento corrompido.

Código	Campo	Descrição
VCCO	ID VCS	O nome do VCS que contém o bloco corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido codificado de apagamento.
CCID	Código bloco	O identificador do fragmento codificado de apagamento corrompido.
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatória, mas não é relevante para esta mensagem em particular. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando TLS (Transport Layer Security) falhou.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP sobre a qual a autenticação falhou.

Código	Campo	Descrição
RUIDA	Identidade do usuário	Um identificador dependente do serviço que representa a identidade do utilizador remoto.
RSLT	Código de motivo	<p>O motivo da falha:</p> <p>SCNI: Falha no estabelecimento de conexão segura.</p> <p>CERM: O certificado estava ausente.</p> <p>CERT: Certificado inválido.</p> <p>CERE: O certificado expirou.</p> <p>CERR: O certificado foi revogado.</p> <p>CSGN: A assinatura do certificado era inválida.</p> <p>CSGU: O signatário do certificado era desconhecido.</p> <p>UCRM: As credenciais do usuário estavam ausentes.</p> <p>UCRI: As credenciais do usuário eram inválidas.</p> <p>UCRU: As credenciais do usuário não foram permitidas.</p> <p>TOUT: A autenticação expirou.</p>

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e a lógica adicional incorporada ao serviço. Se esta autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, é registada uma mensagem de auditoria. Isso permite consultas para tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota ter uma configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Essa mensagem de auditoria deve ser monitorada para detetar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera essa mensagem de auditoria quando um serviço atualizou ou registrou informações sobre si mesmo no sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: <ul style="list-style-type: none"> • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID de nó	O ID do nó do serviço que iniciou a solicitação de atualização.
GNTTP	Tipo de dispositivo	O tipo de dispositivo do nó de grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A cadeia de caracteres que identifica a versão do modelo do dispositivo do nó de grade no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consulta de serviço).
GNIA	Endereço IP	O endereço IP do nó da grade.

Essa mensagem é gerada sempre que um nó de grade atualiza sua entrada no Grid Nodes Bundle.

GNUR: GNDS Unregistration

O serviço CMN gera essa mensagem de auditoria quando um serviço tem informações não registradas sobre si mesmo a partir do sistema StorageGRID.

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: <ul style="list-style-type: none"> • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID de nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grelha terminada

Esta mensagem de auditoria indica que o serviço CMN terminou de processar a tarefa de grade especificada e moveu a tarefa para a tabela Histórico. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria Grid Task Started correspondente. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	Código tarefa	<p>Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa de grade seja gerenciada ao longo de seu ciclo de vida.</p> <p>Observação: o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.</p>

Código	Campo	Descrição
RSLT	Resultado	<p>O resultado final do status da tarefa de grade:</p> <ul style="list-style-type: none"> • SUCS: A tarefa de grade foi concluída com sucesso. • ABRT: A tarefa de grade foi cancelada sem um erro de reversão. • ROLF: A tarefa de grade foi cancelada e não foi possível concluir o processo de reversão. • CANC: A tarefa de grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como uma duplicata.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem de tarefa de Grade enviada para tarefas de grade iniciadas pelo serviço de envio de tarefa de Grade interno e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela pendente, essa mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	Código tarefa	<p>Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida.</p> <p>Observação: o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.</p>
RSLT	Resultado	<p>O resultado. Este campo tem apenas um valor:</p> <ul style="list-style-type: none"> • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grelha enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	Código tarefa	<p>Identifica de forma única uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida.</p> <p>Observação: o ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, neste caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria enviadas, iniciadas e encerradas.</p>
TTYT	Tipo tarefa	O tipo de tarefa de grade.

Código	Campo	Descrição
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição tarefa	Uma descrição humanamente legível da tarefa de grade.
CUBAS	Válido após Timestamp	A primeira vez (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do Timestamp	A última hora (UINT64 microssegundos a partir de 1 de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A origem da tarefa: <ul style="list-style-type: none"> • TXTB: A tarefa de grade foi enviada pelo sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada através do Serviço interno de envio de tarefa de Grade.
ACTV	Tipo de ativação	O tipo de ativação: <ul style="list-style-type: none"> • AUTO: A tarefa de grade foi submetida para ativação automática. • PEND: A tarefa de grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.
RSLT	Resultado	O resultado da submissão: <ul style="list-style-type: none"> • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: ILM iniciou Excluir

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis:** Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis ou contentores Swift.** Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento na política ILM ativa se aplica atualmente ao objeto.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CMPA	Conformidade: Eliminação automática	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o intervalo esteja sob uma retenção legal.
CMPL	Conformidade: Guarda legal	Apenas para objetos em buckets compatíveis com S3. 0 (falso) ou 1 (verdadeiro), indicando se o balde está atualmente sob uma retenção legal.
CMPR	Conformidade: Período de retenção	Apenas para objetos em buckets compatíveis com S3. O comprimento do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Apenas para objetos em buckets compatíveis com S3. O tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do intervalo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em buckets não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCALIZAÇÃO	Locais	<p>O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído).</p> <p>CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto.</p> <p>CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto.</p> <p>CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.</p>
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
RSLT	Resultado	<p>O resultado da operação ILM.</p> <p>SUCS: A operação ILM foi bem-sucedida.</p>
REGRA	Etiqueta de regras	<ul style="list-style-type: none"> • Se um objeto em um bucket compatível com S3 estiver sendo excluído automaticamente porque seu período de retenção expirou, esse campo estará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se aplicam atualmente ao objeto, este campo mostra o rótulo legível por humanos da última regra ILM aplicada ao objeto.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

LKCU: Limpeza de objetos sobrescritos

Essa mensagem é gerada quando o StorageGRID remove um objeto sobrescrito que antes era necessário limpar para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 ou Swift grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	<i>Somente uso interno.</i>
LUID	UUUID Objeto removido	O identificador do objeto que foi removido.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
UUID	Identificador universal único	O identificador do objeto que ainda existe. Este valor só está disponível se o objeto não tiver sido excluído.

LLST: Localização perdida

Essa mensagem é gerada sempre que um local para uma cópia de objeto (replicado ou codificado de apagamento) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBID	O CBID afetado.
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
UUID	ID universal única	O identificador do objeto afetado no sistema StorageGRID.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por apagamento. A ID do perfil de codificação de apagamento utilizado.

Código	Campo	Descrição
LTYP	Tipo de localização	CLDI (Online): Para dados de objeto replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
PCLD	Caminho para o objeto replicado	O caminho completo para a localização do disco dos dados do objeto perdido. Somente retornado quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Toma a forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Resultado	Sempre NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de acionamento	UTILIZADOR: Utilizador acionado SIST: Sistema acionado

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento Registra as solicitações do usuário para a API de gerenciamento. Cada solicitação que não é uma solicitação GET ou HEAD para a API Registra uma resposta com o nome de usuário, IP e tipo de solicitação para a API.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome de domínio do host.
MPAT	PATH da solicitação	O caminho da solicitação.

Código	Campo	Descrição
MPQP	Parâmetros de consulta de solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo do pedido	<p>O conteúdo do corpo do pedido. Enquanto o corpo da resposta é registrado por padrão, o corpo da solicitação é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo de resposta, elas são retiradas do corpo de solicitação para os seguintes métodos POST:</p> <ul style="list-style-type: none"> • Nome de usuário e ID de conta em POST authorize • Nova configuração de sub-redes em POST /grid/grid-networks/update • Novos servidores NTP em POST /Grid/ntp-server/update • IDs de servidor desativadas em POST /Grid/Servers/Deactivation <p>Nota: as informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).</p>
MRMD	Método de solicitação	<p>O método de solicitação HTTP:</p> <ul style="list-style-type: none"> • POST • COLOQUE • ELIMINAR • PATCH
MRSC	Código de resposta	O código de resposta.

Código	Campo	Descrição
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. Nota: as informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN de utilizador	A URNA (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna bem-sucedido (SUCS) ou o erro relatado pelo back-end.

OLST: O sistema detetou Objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar cópias de um objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O CBID do objeto perdido.
NOID	ID de nó	Se disponível, a última localização direta ou nearline conhecida do objeto perdido. É possível ter apenas o ID do nó sem um ID de volume se as informações do volume não estiverem disponíveis.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	Se disponível, o nome do bucket S3 e o nome da chave S3 ou o nome do contentor Swift e o identificador do objeto Swift.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

Código	Campo	Descrição
UUID	ID universal única	O identificador do objeto perdido dentro do sistema StorageGRID.
VOLI	ID do volume	Se disponível, o ID de volume do nó de armazenamento ou nó de arquivo para a última localização conhecida do objeto perdido.

ORLM: Regras Objeto cumpridas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras ILM.



A mensagem ORLM não é gerada quando um objeto é armazenado com êxito pela regra de fazer cópias 2 padrão se outra regra na política usar o filtro avançado tamanho do objeto.

Código	Campo	Descrição
BUID	Colhedor do balde	Campo ID do balde. Usado para operações internas. Aparece apenas se STAT for PRGD.
CBID	Identificador do bloco de conteúdo	O CBID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCALIZAÇÃO	Locais	O local de armazenamento de dados de objetos no sistema StorageGRID. O valor para LOCS é "" se o objeto não tiver locais (por exemplo, ele foi excluído). CLEC: Para objetos codificados por apagamento, o ID do perfil de codificação de apagamento e o ID do grupo de codificação de apagamento que é aplicado aos dados do objeto. CLDI: Para objetos replicados, o ID do nó LDR e o ID do volume da localização do objeto. CLNL: ARC node ID da localização do objeto se os dados do objeto forem arquivados.
CAMINHO	S3 Bucket/Key ou Swift Container/Object ID	O nome do bucket S3 e o nome da chave S3, ou o nome do contentor Swift e o identificador de objeto Swift.

Código	Campo	Descrição
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível por humanos dado à regra ILM aplicada a este objeto.
SEGC	UUID do recipiente	UUID do recipiente para o objeto segmentado. Este valor só está disponível se o objeto estiver segmentado.
SGCB	CBID do recipiente	CBID do recipiente para o objeto segmentado. Este valor está disponível apenas para objetos segmentados e multipartes.
STAT	Estado	O estado da operação ILM. Feito: Operações ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação ILM. PRGD: O objeto foi excluído do sistema StorageGRID. NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID. Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.

A mensagem de auditoria ORLM pode ser emitida várias vezes para um único objeto. Por exemplo, ele é emitido sempre que um dos seguintes eventos ocorrer:

- As regras de ILM para o objeto são satisfeitas para sempre.
- As regras de ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano deteta que uma cópia dos dados de objetos replicados está corrompida. O sistema StorageGRID executa uma avaliação ILM para substituir o objeto corrompido.

Informações relacionadas

- [Transações de ingestão de objetos](#)
- [Eliminar transações](#)

OVWR: Substituição de objetos

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo (novo)	O CBID para o novo objeto.
CSIZ	Tamanho Objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.
OCBD	Identificador de bloco de conteúdo (anterior)	O CBID para o objeto anterior.
UUID	ID universal única (novo)	O identificador do novo objeto dentro do sistema StorageGRID.
OID	ID universal única (anterior)	O identificador para o objeto anterior dentro do sistema StorageGRID.
CAMINHO	S3 ou Swift Object Path	O caminho de objeto S3 ou Swift usado para o objeto anterior e novo
RSLT	Código do resultado	Resultado da transação de Sobreposição de objetos. O resultado é sempre: SUCS: Bem-sucedido
SGRP	Local (Grupo)	Se presente, o objeto sobrescrito foi excluído no local especificado, que não é o local onde o objeto sobrescrito foi ingerido.

ADICIONAR: Desativação da auditoria de segurança

Essa mensagem indica que o serviço de origem (ID do nó) desativou o Registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para desativar a auditoria.

Código	Campo	Descrição
AEUN	Nome de utilizador	O nome de usuário que executou o comando para desativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente ativado, mas agora foi desativado. Normalmente, isso é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SADE: Ativação da auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registo de mensagens de auditoria; as mensagens de auditoria estão novamente a ser recolhidas e entregues.

Código	Campo	Descrição
AETM	Ativar método	O método utilizado para ativar a auditoria.
AEUN	Nome de utilizador	O nome de usuário que executou o comando para ativar o log de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NENHUM é usado em vez DE SUCS para que esta mensagem não seja filtrada.

A mensagem implica que o registo foi anteriormente desativado (SADD), mas foi agora restaurado. Isso geralmente é usado apenas durante a ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desativar a auditoria é então permanentemente bloqueada.

SCMT: Confirmação de armazenamento de objetos

O conteúdo da grade não é disponibilizado ou reconhecido como armazenado até que ele tenha sido comprometido (ou seja, ele foi armazenado persistentemente). O conteúdo armazenado persistentemente foi completamente gravado no disco e passou

por verificações de integridade relacionadas. Essa mensagem é emitida quando um bloco de conteúdo é comprometido com o armazenamento.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com o armazenamento permanente.
RSLT	Código do resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 DELETE

Quando um cliente S3 emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou bucket especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em buckets não incluem este campo.
DMRK	Eliminar ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket com versão. As operações em buckets não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anônimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.

Código	Campo	Descrição
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para pedidos anônimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 GET

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.

Código	Campo	Descrição
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RANG	Leitura de intervalo	Apenas para operações de leitura de gama. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho de todo o objeto.
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.

Código	Campo	Descrição
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anônimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: urn:sgws:identity::03393893651506583485:root Vazio para pedidos anônimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: S3 CABEÇA

Quando um cliente S3 emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anônimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para pedidos anônimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.

Código	Campo	Descrição
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: S3 POST

Quando um cliente S3 emite uma solicitação POST Object, essa mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da solicitação de restauração PÓS-objeto. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável. Defina como "elecionar" para uma operação S3 Select.
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.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	Restaurar informações.

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CMPS	Definições de conformidade	As configurações de conformidade usadas ao criar o bucket, se estiverem presentes na solicitação PUT Bucket (truncada para os primeiros 1024 caracteres)

Código	Campo	Descrição
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se estiver presente na solicitação.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LKEN	Bloqueio Objeto ativado	Valor do cabeçalho da solicitação x-amz-bucket-object-lock-enabled , se estiver presente na solicitação COLOCAR balde.
LKLH	Bloqueio Objeto retenção legal	Valor do cabeçalho da solicitação x-amz-object-lock-legal-hold , se estiver presente na solicitação COLOCAR Objeto.
LKMD	Modo de retenção de bloqueio de objetos	Valor do cabeçalho da solicitação x-amz-object-lock-mode , se estiver presente na solicitação COLOCAR Objeto.
LKRU	Reter Data até bloqueio Objeto	Valor do cabeçalho da solicitação x-amz-object-lock-retain-until-date , se estiver presente na solicitação COLOCAR Objeto.
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	S3KY	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
S3SR	S3 Subrecurso	O bucket ou o subrecurso do objeto em que está sendo operado, se aplicável.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anônimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SRCF	Configuração de sub-recurso	A nova configuração de subrecursos (truncada para os primeiros 1024 caracteres).

Código	Campo	Descrição
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para pedidos anónimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UID	ID de carregamento	Incluído apenas nas mensagens SPUT para operações de Upload de várias partes completas. Indica que todas as peças foram carregadas e montadas.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	A ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de controle de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "Habilitado" ou "suspense". As operações em objetos não incluem este campo.

SREM: Armazenamento de objetos Remove

Essa mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não é mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código do resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Essa mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

SUPD: S3 metadados atualizados

Essa mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização de metadados for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de ligação	O identificador de sistema exclusivo para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em buckets não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	S3 ID da conta do locatário (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	S3 ID da chave de acesso (remetente do pedido)	O código de chave de acesso S3 hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anônimos.
SAIP	Endereço IP (remetente do pedido)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.

Código	Campo	Descrição
SBAI	S3 ID da conta do locatário (proprietário do balde)	O ID da conta do locatário do proprietário do bucket alvo. Usado para identificar acesso entre contas ou anônimo.
SUSR	S3 URNA do usuário (solicitar remetente)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O utilizador pode ser um utilizador local ou um utilizador LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para pedidos anônimos.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
VSID	ID da versão	O ID da versão da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SVRF: Falha na verificação do armazenamento de objetos

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que os dados de objeto replicados são lidos ou gravados no disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente ingeridos no sistema. Se alguma dessas verificações falhar, o sistema coloca automaticamente em quarentena os dados de objeto replicados corrompidos para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou a verificação.
RSLT	Código do resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação HMAC (hash-based message Authentication code). EHSB: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. PERR: Estrutura inválida do arquivo de disco. DERR: Erro de disco. FNAM: Nome de arquivo ruim.

Nota: esta mensagem deve ser monitorada de perto. Falhas na verificação de conteúdo podem indicar tentativas de adulteração de conteúdo ou falhas iminentes de hardware.

Para determinar que operação acionou a mensagem, consulte o valor do campo AID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação do armazenamento de objetos desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detetada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do ficheiro	O caminho do arquivo da cópia de objeto inesperada.

Código	Campo	Descrição
RSLT	Resultado	Este campo tem o valor 'NONE'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

Nota: a mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objetos foram detetadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar tentativas de adulteração de conteúdo ou falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, esta mensagem é enviada apenas após um reinício subsequente, porque a fila de mensagens de auditoria não é eliminada antes do encerramento. Procure a mensagem DO SISTEMA, enviada no início da sequência de encerramento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SIST: Paragem do nó

Quando um serviço é parado graciosamente, essa mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. O SYST pode ser usado para determinar se o desligamento foi solicitado, antes que o serviço seja reiniciado (ao contrário do SYSD, que normalmente é enviado após o reinício do serviço).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem DO SISTEMA não pode indicar um desligamento "sujo", porque a mensagem é

gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, essa mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Limpar encerramento	A natureza do desligamento: SUCS: O sistema foi desligado de forma limpa. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte a descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (uma vez que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Server Manager reinicia automaticamente um serviço com falha.

VLST: Volume iniciado pelo usuário perdido

Esta mensagem é emitida sempre que o `/proc/CMSI/Volume_Lost` comando é executado.

Código	Campo	Descrição
VOLL	Identificador de volume inferior	A extremidade inferior do intervalo de volume afetado ou um único volume.
VOLU	Identificador de volume superior	A extremidade superior do intervalo de volume afetado. Igual a VOLL se um único volume.
NOID	Código nó origem	O ID do nó no qual os locais foram perdidos.
LTYP	Tipo de localização	'CLDI' (Online) ou 'CLNL' (Nearline). Se não for especificado, o padrão é 'CLDI'.

Código	Campo	Descrição
RSLT	Resultado	Sempre "NENHUM". RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NENHUM' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

WDEL: Swift DELETE

Quando um cliente Swift emite uma transação DE EXCLUSÃO, uma solicitação é feita para remover o objeto ou contentor especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação DE EXCLUSÃO. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Local (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o local onde o objeto foi ingerido.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.

Código	Campo	Descrição
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WGET: Rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contentor ou listar os contentores em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e contêineres não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e contêineres não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).

Código	Campo	Descrição
RSLT	Código do resultado	Resultado da TRANSAÇÃO GET. O resultado é sempre SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e contêineres não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA rápida

Quando um cliente Swift emite uma TRANSAÇÃO PRINCIPAL, uma solicitação é feita para verificar a existência de uma conta, contentor ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contas e contêineres não incluem esse campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contas e contêineres não incluem esse campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código do resultado	Resultado da TRANSAÇÃO PRINCIPAL. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.

Código	Campo	Descrição
WCON	Contentor Swift	O nome do contentor Swift. As operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contas e contêineres não incluem esse campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: Swift PUT

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contentor. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador do bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo é definido como 0. As operações em contentores não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. As operações em contentores não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalho de solicitação HTTP registrados, conforme selecionado durante a configuração. Nota: X-Forwarded-For é incluído automaticamente se estiver presente na solicitação e se o X-Forwarded-For valor for diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).

Código	Campo	Descrição
MTME	Hora da última modificação	O timestamp Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código do resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da camada 7, o endereço IP do balanceador de carga.
UUID	Identificador universal único	O identificador do objeto dentro do sistema StorageGRID.
WACC	ID da conta Swift	O ID exclusivo da conta, conforme especificado pelo sistema StorageGRID.
WCON	Contentor Swift	O nome do contentor Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. As operações em contentores não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

Informações sobre direitos autorais

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 INTERRUPTÃO 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.